# ROLE OF MULTIMEDIA INFORMATION RETRIEVAL IN PROVIDING A CREDIBLE EVIDENCE FOR DIGITAL FORENSIC INVESTIGATIONS: OPEN SOURCE INTELLIGENCE INVESTIGATION ANALYSIS

Amr Adel[1] and Brian Cusack[2]

[1]Whitecliffe College of Technology & Innovation, Auckland, New Zealand
[2]Cyber Forensics Research Centre, Auckland University of Technology, Auckland, New Zealand

***ABSTRACT***

*Enhancements in technologies and shifting trends in customer behaviour have resulted in an increase in the variety, volume, veracity and velocity of available data for conducting digital forensic analysis. In order to conduct intelligent forensic investigation, open source information and entity identification must be collected. Challenge of organised crimes are now involved in drug trafficking, murder, fraud, human trafficking, and high-tech crimes. Criminal Intelligence using Open Source Intelligence Forensic (OSINT) is established to perform data mining and link analysis to trace terrorist activities in critical. In this paper, we will investigate the activities done by a suspect employee. Data mining is to be performed and link analysis as well to confirm all participating parties and contacted persons used in the communications. The proposed solution was to identify the scope of the investigation to limit the results, ensure that expertise and correct tools are ready to be implemented for identifying and collecting potential evidences. This enhanced information and knowledge achieved are of advantage in research. This form of intelligence building can significantly support real world investigations with efficient tools. The major advantage of analysing data links in digital forensics is that there may be case-related information included within unrelated databases.*

***KEYWORDS***

*Open Source Intelligence, Information Retrieval,Digital Forensics, Cyber-Crimes & Data Mining.*

## 1. INTRODUCTION

Increasing the volume of digital forensic data has been defined as a challenge to forensic examiners and investigators due to diversity of devices, and services that play an important role in collecting digital evidence. This variety of data sources poses challenging issues to forensic investigators from identifying system's specifications and storage capacity, processing data acquisition, and analysing the acquired evidence, then reporting these evidence into a technical report for to be encountered by law enforcement agencies [1].

Five major problems have been outlined for digital forensics in different areas; these areas can be categorised as complexity problem, diversity problem, consistency and correlation problem, volume problem, and unified time lining problem [2]. The complexity problem is acquiring data

David C. Wyld et al. (Eds): CCSEA, BIoT, DKMP, CLOUD, NLCAI, SIPRO - 2020
pp. 11-22, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101002

at its lowest format with a serious increase of data volumes during the process, which needs for sophisticated techniques for reducing/filtering data prior the analysis. The diversity problem results from the lack of investigating and examining standard techniques in order to be able to examine the increasing number of data source types. This lack of standardization for adding different types of formats into the investigation process is causing a complexity of sharing the digital evidence between the international law enforcement agencies that are trained by Digital Forensic Training Program to deal with triage files [3]. The problem of consistency and correlation is resulting from static function of existing forensics tools that are designed to catch fragments of evidence, which is considered as limitation and there is a need to perform other sophisticated functions to assist forensic investigators. The problem of data volume comes from the lack of automation tools that can handle effectively the large number of data volumes in data storages and the electronic devices that store information. The problem of unified time lining results from having multiple data sources came from different time zones, which needed as documented reference and changes in timestamp and clocks.

This paper is organized as follows; section 2 discusses digital forensic environment's challenges as well as classifications of data acquisition sources; section 3 analyses the digital forensic gap of critical infrastructures; section 4 demonstrates the implementation and analysis of an example of open-source intelligence tool. In section 5, we conclude to point some of recent issues to be investigated in the future.

## 2. RELATED WORK

Due to the sensitive nature of this data, forensic investigators and examiners will have to apply advanced procedures into consideration for to follow in order to acquire the data. Additionally, practices needed to be implemented carefully prior the process of acquiring data in order to maintain its admissibility. Figure 1 illustrates the life cycle of large amounts of data in critical infrastructures.

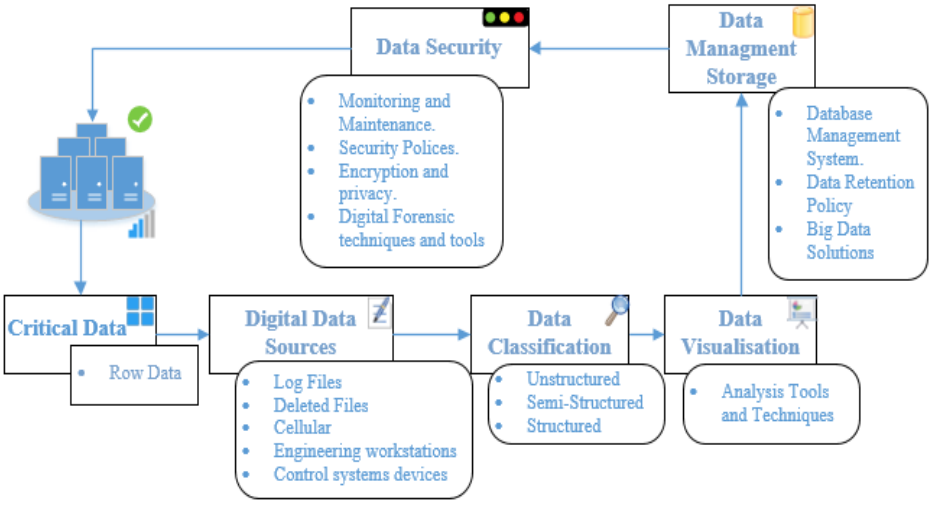



Figure 1. Large amounts of Data Life Cycle

Most sensitive data acquisition scenarios are experiencing the three V – they are high volume, high velocity, and high variety, with low data value [4]. Therefore, data acquisition is vital. Data Acquisition is the process of gathering and filtering information from all possible sources for to be analysed in order to make the first task of forensic investigation. Technically, data acquisition

tends to collect digital evidence from all potential electronic media. For successfully undertaking this task, forensic examiners and investigators have to differentiate between the two types of data acquisition, which are live acquisition and static acquisition in order to find the suitable method of collecting the evidence based on the case status [5].

Due to the sophistication of Internet of Things, cloud computing, and distributed computing that are handling large volumes of data in critical systems, forensic investigators are experiencing a number of challenges in order to initialise with the first stage, which is data acquisition. Some of these challenges are data complexity, computational complexity, and system complexity [6]. The development of complex data has supported us with exceptional large-scale trials when dealing with computational problems.

Data Acquisition's major function in digital forensic investigations is to provide copies of original drives. This procedure has to be done on the original drive in order to ensure that there is another copy in case the original drive corrupted or damaged [6]. This process could be done acquiring volatile and non-volatile data. A volatile data is the data that has been stored in live system and when shutting down the device, the data will be lost. Control system status, device memory, network connections and time clocks, command history, and processes running are some of volatile data [7]. Non-volatile data is a concept that aims to keep data unchanged while computers powered off, which means data is in a stable place. Hard drives or Virtual drives such as Google drive can recover certain types of stored data and deleted files after the user has accessed his data whether his computer directly or through web browser [1]. For instance, emails, sheets saved on the computer, or pictures. In addition, there are other sources to find non-volatile data such as local drives, smart phones, shared folder, and USB thumb drives [8]. Often, during the examination process of forensic investigation, investigators collect all information from non-volatile data to use them a credible evidence of the incident.

In order to handle digital evidence and conduct successful forensic investigations, sub-functions of data acquisition will need to be identified to forensic examiners and investigators. Data acquisition sub-functions can be classified as follows:

1. Physical Data Copy
2. Logical Data Copy
3. Data Acquisition Format
4. Command Line Acquisition

Forensic tools function can assist forensic investigators to extract and acquire data based on the above data acquisition sub-functions category. Table 1 shows the comparison between the sub-functions and tools used in forensic investigation.

Table 1: Comparison between forensic tools and sub-functions [6].

| Function | ProDiscover Basic | OSForensics, demo version | AccessData FTK | Guidance Software EnCase |
|---|---|---|---|---|
| **Acquisition** | | | | |
| Physical data copy | ✓ | ✓ | ✓ | ✓ |
| Logical data copy | ✓ | ✓ | ✓ | |
| Data acquisition formats | ✓ | ✓ | ✓ | ✓ |
| Command-line processes | | | | ✓ |
| GUI processes | ✓ | ✓ | ✓ | ✓ |
| Remote acquisition | | ✓ | ✓ | ✓ |

## 2.1. Incident Response Team

The arrangement for establishing an incident response team is essential and will have to be take into consideration especially in industrial control systems. The training and skills required for establishing this team are in different areas that can include control system engineering, digital forensics, and IT incident response. At least one member of the team must have in-depth knowledge and at least one member must have a basic knowledge of these skilful areas [13]. For instance, basic knowledge in control system engineering, digital forensics, and IT incident response will be required by a system engineer, while having an expert-level of understanding in control systems. A combination of technical skills provides high-level of understanding for finding holes, vulnerabilities, and tackling a numerus types of threats. Effective forensic research should minimize the noise and maximise the context in order to have investigative information as shown in figure 2. Training for those specialised engineers are crucial to keep their knowledge updated and fresh [14].

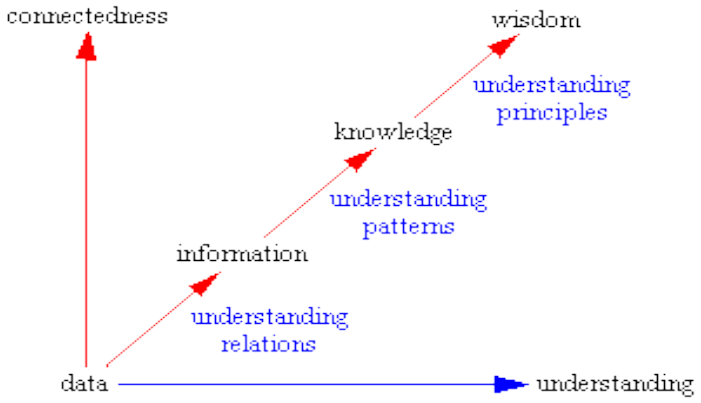



Figure 2: Knowledge Management Understanding Hierarchy [4]

In working environments, safety procedures have to be provided to the incident response team in order to allow them taking correct actions when dealing with critical incidents in order to handle security attacks [15]. For that reason, this is must be the first consideration. In addition, each member of incident response team must receive the appropriate training in safety requirements and operational procedures of the industrial control systems to be well qualified in their positions.

## 2.2. Volatile Evidence Preservation

A volatile data is the data that has been stored in live system and when shutting down the device, the data will be lost. Volatile data can be collected from control system status, device memory, network connections and time clocks, command history, and processes running [7]. Record and capture all types of displays such as LCDs or any device which capable of making screenshots. Moreover, if feasible, videos and photos can be recorded as well. This is to capture and record all light status, for example, status lights (on, off, flashing). This is could be useful during the investigation process for identifying actions performed before the incident. Obtain as much as possible information from targeted memory of devices. The process of obtaining information from the devices' memory will require different tools and the necessary knowledge to use these tools effectively to retrieve all data [10]. Environments that working with PLCs must have the capability to capture all "data files" from configurations workstations and Ladder Logic Programs can be transferred from PLC to the workstations and preserved as well as a part of forensic examination. Acquire data and time that could be traced by network connections such as IP addresses, and port numbers. All relevant traffic data can be captured by open source and

commercial applications to perform network reconnaissance [5]. Time and date in many cases are a treasure. The capability of getting time clocks for each performed action can assist in tracing the incident and will allow forensic investigators to design an accurate timeframe for collecting particular evidence [1]. On a suspicious system, reviewing the command history can give forensic examiners a brief about the recent activities that have been done. It also can serve an audit trails for extending as possible in the process of investigating the target machines. In addition, processes running can give a good review to show a full list of all processes running on the suspicious machine [9]. This reviewing will help examiners in detecting malicious process and abnormal activities.

## 2.3. Non-Volatile Evidence Preservation

The concept of non-volatile data is to keep data unchanged while computers powered off, which means data is in a stable place. Hard drives or Virtual drives such as Google drive can recover certain types of stored data and deleted files after the user has accessed his data whether his computer directly or through web browser [1]. For instance, emails, sheets saved on the computer, or pictures. In addition, there are other sources to find non-volatile data such as local evidence drives, cloud storage, shared folder on a local network, smart phones, PDAs, and USB thumb drives [8]. Often, during the examination process of forensic investigation, investigators collect all information from non-volatile data to use them a credible evidence of the incident.

Temporary files are some of credible evidence that could be collected during the process of forensic investigation. Temporary file is created by programs when there are no places for allocating memory blocks for the tasks. These files are usually deleted after closing the program, but sometimes there are some files keep their temporary files in the computer. Windows registry is one of powerful evidence forensic investigators can collect. The registry is created database for the system containing all system's information such as user's preferences, settings for hardware/software, and operating system priority in case the computer has multiple operating systems [16].

Logging event is also effective evidence used to collect event's information about the system's transactions that have been made by registered users to be analysed and assessed for its admissibility [17].

Boot sectors could be vital in the forensic process investigation. It can provide all instructions about booting operating systems. This is because hard drives usually partitioned into several partitions, and each of these partitions may has a different operating system. For example, when computer powered on, it offers a user an option to choose between two operating systems, one of them Windows 7 and the other one is Ubuntu.

History of web browsers and cookies are also a valuable addition to the forensic report. During the forensic process, web History can provide user search for keywords, websites, or saved login credentials that could lead to sensitive information such as online purchases and bank accounts [12]. Furthermore, downloaded contents will still be remaining in the hard drive until the user delete it, often, these contents still exist in unallocated space of the hard drive. This could assist in tracing the incident faster.

## 2.4. Forensic Challenge with Collection

Operational process of forensics collection in normal environments require understanding the severity nature of cyber forensic incidents and addressing a number of challenges that forensic investigators encounter during the process of examination such as limitations of cultures, poor

administrations, volatile memory, and insufficient logging systems [18]. In industrial control systems, it is difference. There are additional challenges such as automation, volatility of data, and data mingling.

One of these challenges is automation. Control system domain will create key information resources in order to handle the data in the direction that to be applied of data retention which is not a requirement and not cost-effective. Volatility of is the other challenge that forensic investigators face and his makes the process of collecting data inviable because the data within the collection process is removed, deleted, or overwritten, and this can make it impossible to be detected in its original state [8]. Furthermore, most examiners are facing another problem in retrieving data forensically, which known as "Data Mingling" [3]. Data Mingling is a serious problem of data mixture and being indistinguishable. Often, the sample of total data investigated in the forensic process is comprised of both data related to the incident and data unrelated to the incident. In order to classify the data, a solution for this problem is presented, which is to attribute unrelated data to inadequate functions labels.

Research has confirmed that the most vital asset to an attacker could be devices that control the infrastructures such as field devices in control systems. It is now important to consider information resources security and its capabilities and access levels in control systems in regards of data retention [16]. The study of understanding how these capabilities can support in forensic investigation should be taking into consideration.

## 2.5. Forensic Challenge in Data Analysis

There are clear solutions for the forensic issue in critical infrastructures, which can adapt those in industrial control systems; however, cyber-forensic and anti-forensic tools have not proved that efficiency in certain areas of computing environments such as data identification, time mismatch, multi-tenancy, owner of data, live forensics, privacy, mobile operating systems, multiple cloud service providers. [11]. Sophisticated tools such as those that copy processes, examine evidence, analyse program for generating checksums in order to complete the verification may not fit perfectly to some of control systems technologies. Consequently, many of digital forensic tools in different areas such as network forensics, database forensics, computer forensics, and mobile forensics will not be able to fit to operate in the newest physical and virtual systems in computing environments such in cloud computing environments [15].

Therefore, digital forensics vendors will have to apply new modifications on their software and frameworks in order to fill the gap and meet the challenge. A core component is the backbone of any forensic ability. The major function of each one of these core components is to make sure that environments can correctly review the necessary information that has been collected for review. The problem comes when the investigator has only one or two sources for extracting the information. This can limit and affects the overall performance in collecting data for analysis [13]. Therefore, it is vital to understand how important to have numerus resources before the domain comes critical.

## 2.6. Forensic Challenge in Reporting

The involvedness of critical infrastructures especially in control systems environments along with its installations, and drives configurations make the process of documentation of these components complex to forensic investigators. Therefore, the documentation must be presented in order identify all evidence acquisitioned into a one report.

Documentation is principal ensure the success of any forensic investigations in control systems environments. Assertive steps should be followed and taken into consideration from the beginning for reporting the crime to closure case [19]. Assets' owners will have to take another several steps in order to identify and detect any types of changes that could be done during operating system installation, configurations of devices, hardware, or any elements whose modified behaviour may affect the original equipment manufacturers [20]. Moreover, vendors are highly recommended to replicate their modified data with asset owners in order to ensure the credibility of information. Such information must be provided to forensic examiners before getting involved in any forensic activity. Afterwards, forensic examiner will shall note amendments and justify for them accordingly for best practices.

## 3. DIGITAL FORENSICS GAP ANALYSIS

Due to the advancements in cyber area, the use of internet and information technology have dramatically increased. Accordingly, this led to serious cyber-attacks that are targeting critical infrastructures. Digital forensic is chosen for obtaining and investigating all types of digital information including malicious evidence found in suspected systems. This operation is meant to be done for making sure evidence is admissible for to be presented to the court. Other reason for performing a formal digital forensic investigation is recovering lost, deleted, or corrupted critical data. The recovered data is a great assist to prosecute the criminals [8].

Formally, sensitive data is an interesting target and is vulnerable to data leakage attack [10]. Digital forensic investigation can help forensic investigators to obtain critical data, such as cluster properties, file retrieval, logging files, metadata, and transaction logs.

In traditional forensic investigations, the forensic investigators are relying on static techniques to remove hard disks and time consuming for acquiring the data. However, a number of architectural and technical limitations have prevented investigators from performing this type of investigation in larger IT infrastructures such as diversity in events and input sources [11].

The evidence collected from the forensic investigation is the data stored in the digital systems and it could be deleted files, hidden files, metadata, corrupted data, hard drive data, in-memory data, or any other forms of data [9].

The key objective from investigating critical infrastructures forensically is to acquire the data to obtain desired results in a defensible manner against cyber-attacks such as Botnet attack in order to prevent cyber-criminals from controlling the system [12].

Reporting digital forensics findings is one of critical phase in digital forensics, because it depends on the investigated environment components, size, and acquired data sources. This stage of digital forensic investigation is to present and discuss all findings and results resulted from particular investigation to stakeholders who will assess and evaluate the outcome of the investigation.

## 4. IMPLEMENTATION

During the hypotheses and examination phase, the forensic investigator found a number of traces of communications that have been sent to suspicious identities. The open source intelligence forensic testing lab was used to route case three. All software and hardware requirements for the forensic computer have been preserved.

Throughout the search and data collection and examination phases, an open source intelligence application was effectively engaged. The Maltego version 4.1.0 was employed to obtain and examine the data. The suspect user contact information has been acquired and plans were set to test the proposed methodology in the first phase of digital forensic investigation to perform link analysis. Application specifications were confirmed for the evidence collection phase. As shown in figure 2, the system specification is for Windows 10 used in the investigation.

## 4.1. Search & Data Collection

To explore the desired and credible traces for the data collection phase, links analysis and data mining have been implemented in this phase for revealing all possible relationships and links associate to the suspected user. This phase was set to trace machine's activities, and summary of these traces shown in the following figure.

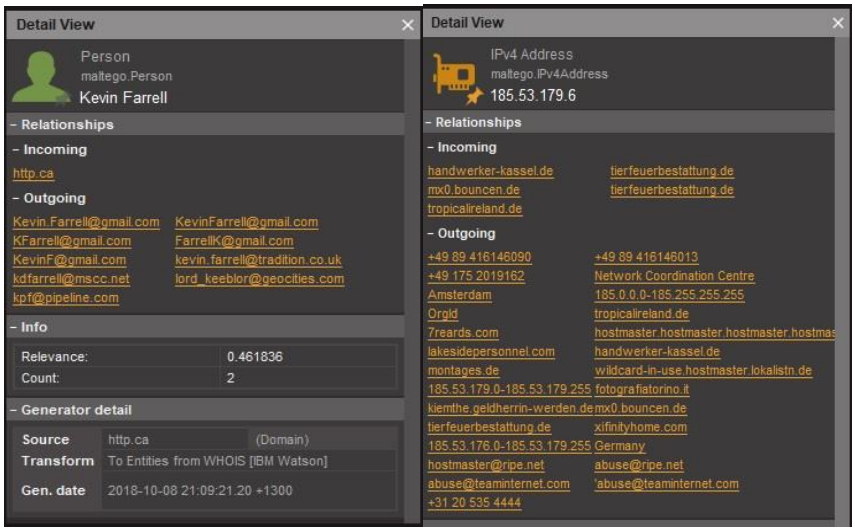



Figure 3: Suspect Email address details

Figure 3 shows all associated communications to the user IP "185.53.179.6". This IP tracing reveal a number of internal communications within the organisation and external communications, which require a deep analysis for the type of communications detected. The figure also shows a number of locations, persons, websites, and net-blocks were involved in his communications, although his role doesn't require dealing with this level of communications. The following phase will conduct a deep linking analysis to examine the metadata linkage found in the above figure.

## 4.2. Examination & Analysis

Examination of the data collected was confirmed based on the clear data collected in the previous phase, which clarify that the user is using his email address to associate with external emails as shown in the figures 4, 5 & 6 and using his external IP address that owned by the organisation for initiating external communications with external bodies. To examine the user activities, data mining and link analyses processes were employed in the phase of search and data collection to confirm the questionably manner of the user.

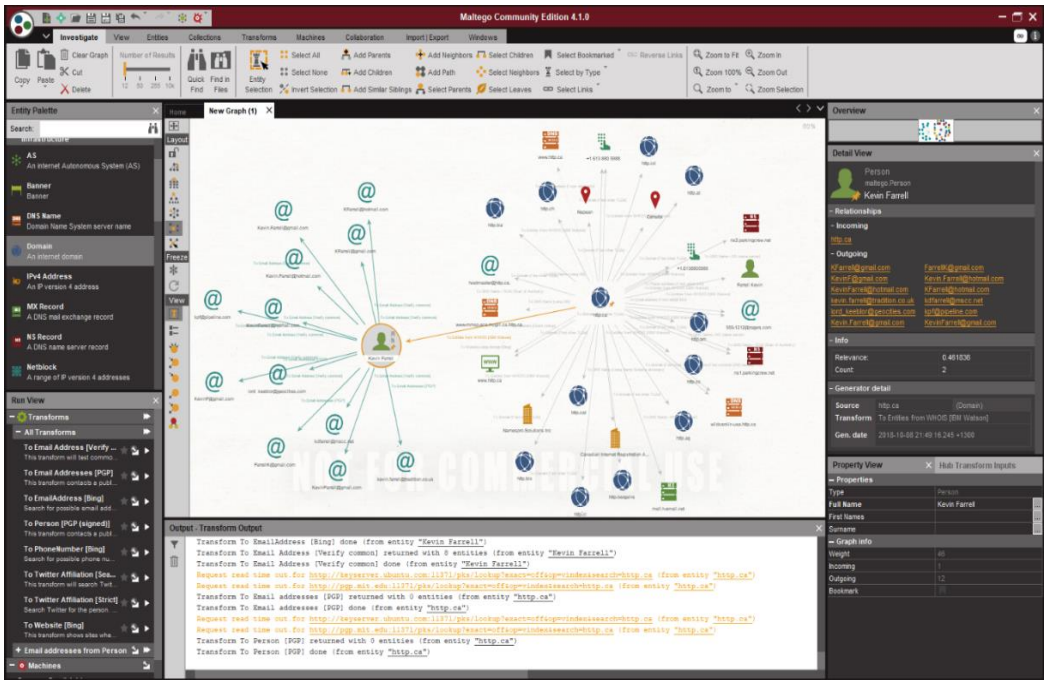



Figure 4: IP Address Link Analysis

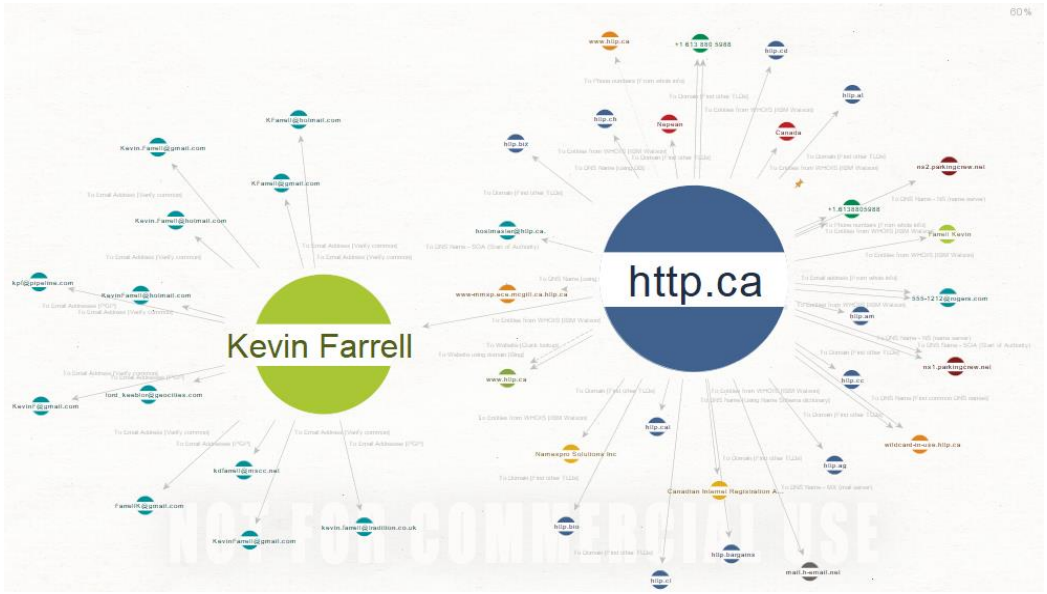
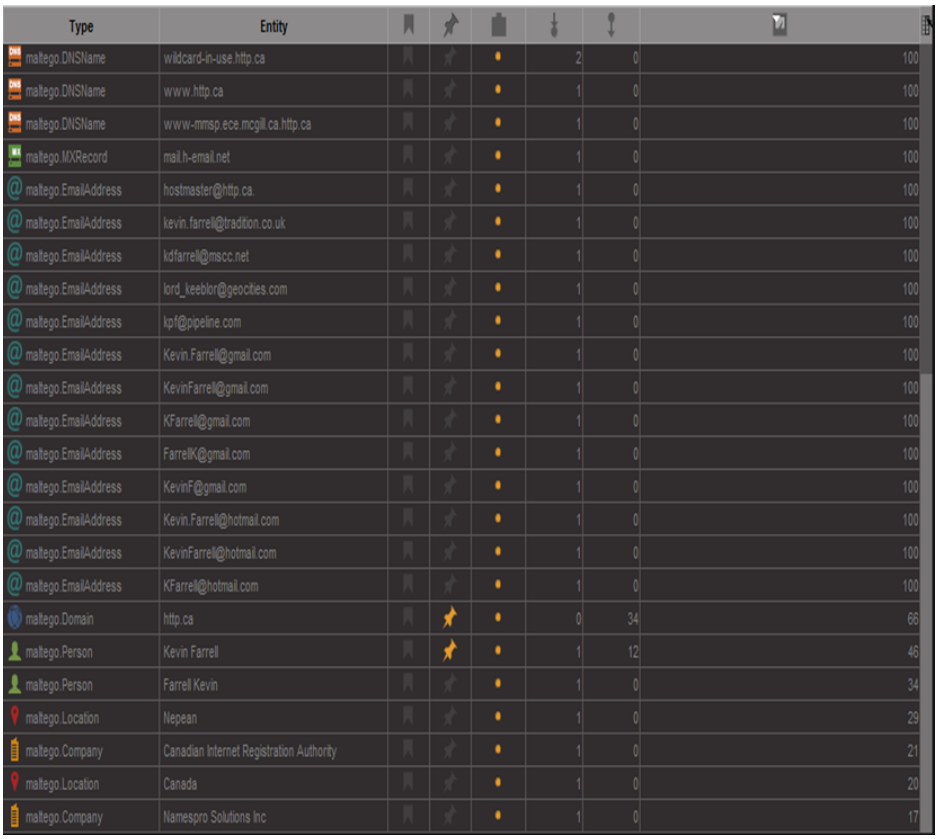



Figure 5: Email Address Link Analysis



| Type | Entity | | | | | | |
|---|---|---|---|---|---|---|---|
| maltego.DNSName | wildcard-in-use.http.ca | | | | 2 | 0 | 100 |
| maltego.DNSName | www.http.ca | | | | 1 | 0 | 100 |
| maltego.DNSName | www-mmsp.ece.mcgill.ca.http.ca | | | | 1 | 0 | 100 |
| maltego.MXRecord | mail.h-email.net | | | | 1 | 0 | 100 |
| maltego.EmailAddress | hostmaster@http.ca. | | | | 1 | 0 | 100 |
| maltego.EmailAddress | kevin.farrell@tradition.co.uk | | | | 1 | 0 | 100 |
| maltego.EmailAddress | kdfarrell@mscc.net | | | | 1 | 0 | 100 |
| maltego.EmailAddress | lord_keeblor@geocities.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | kpf@pipeline.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | Kevin.Farrell@gmail.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | KevinFarrell@gmail.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | KFarrell@gmail.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | FarrellK@gmail.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | KevinF@gmail.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | Kevin.Farrell@hotmail.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | KevinFarrell@hotmail.com | | | | 1 | 0 | 100 |
| maltego.EmailAddress | KFarrell@hotmail.com | | | | 1 | 0 | 100 |
| maltego.Domain | http.ca | | | | 0 | 34 | 66 |
| maltego.Person | Kevin Farrell | | | | 1 | 12 | 46 |
| maltego.Person | Farrell Kevin | | | | 1 | 0 | 34 |
| maltego.Location | Nepean | | | | 1 | 0 | 29 |
| maltego.Company | Canadian Internet Registration Authority | | | | 1 | 0 | 21 |
| maltego.Location | Canada | | | | 1 | 0 | 20 |
| maltego.Company | Namespro Solutions Inc | | | | 1 | 0 | 17 |

Figure 6: Analysed Data Table

Data acquisition is recognised as a relationships inquiry of suspected users by tracing their emails and local IP addresses to reveal credible information such as external emails, external IP address, other domains, DNS records to resolve different IPs to names, MX records to use external emails, persons involved in his communications, and websites. The forensic examination was conducted through extracting system and physical information from the open source intelligence to be able to acquire the desired information. The data examination method has been involved and the system engaged was a windows-based. The above figure shows a sample of detailed information about the parties involved in the communications.

## 5. CONCLUSION

This research identified the gap from the current and updated literature and industrialized a reliable piece of artefact as a key to fill the gap acknowledged. The proposed tool used and it has been evaluated in the designed virtual lab and the testbed was made based on a controlled environment. Additionally, the hypotheses examination showed that the industrialized artefact still requests to be confirmed based on live case in the area. Anti-forensics techniques are the one of most significant research areas presently and in the future. The fast growth in capabilities of information warfare and cyber weapons are supporting a significant challenge to the supervision, and approach that supports critical infrastructures' resources. The chief objective of investigating this flourishing area therefore is to uncover this challenge, expose any mythologies, and support an integrated framework along with the proposed one through which to recognize, assess, and eventually report the evolving cyber-link.

## REFERENCES


[1] Quick, D., & Choo, K. R. (2014). Google Drive: Forensic analysis of data remnants. Journal of Network and Computer Applications, 40, 179-193. https://www.sciencedirect.com/science/article/pii/S1084804513002051?casa_token=FmDXdVZX3EYAAAAA:OPEFKx8bFOqPxT4pXlPhYmpAjf9w53y5jWv1IDq5bBolXXuRYreSnCNFG1AoPakaxCo-PCUmEvU

[2] Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. arXiv preprint arXiv:1604.03850. https://arxiv.org/pdf/1604.03850.pdf

[3] Hitchcock, B., Le-Khac, N., & Scanlon, M. (2016) Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists. Digital Investigation, 13 (S1), 03. https://www.sciencedirect.com/science/article/pii/S1742287616300044

[4] Cavanillas, J. M., Curry, E., & Wahlster, W. (2016). New horizons for a data-driven economy: a roadmap for usage and exploitation of big data in Europe. Springer. http://library.oapen.org/bitstream/id/b82b0e7e-d065-4711-ba4d-a97f974f605d/1002241.pdf

[5] Jin, X., Wah, B. W., Cheng, X., & Wang, Y. (2015). Significance and Challenges of Big Data Research. Big Data Research, Vol. 2(2), 59-64. https://www.sciencedirect.com/science/article/pii/S2214579615000076?casa_token=Fw_Lm2G0Ae0AAAAA:KT0ggnTS9eRevNyjiVGBZnB6kMfRrxv6bafWy7A7ltAYCY5Xis-EwTwqMb4UJUVcWl5hVO5al3Q

[6] Nelson, B., Phillips, A., & Steuart, C. (2016). Guide to computer forensics and investigations: processing digital evidence. Cengage Learning. Boston, USA. https://college.cengage.com/information_security/course360/computer_forensics_9781133134855/ebook/nelson98836_1435498836_02.06_chapter06.pdf

[7] Al-Dhaqm, A., Abd Razak, S., Othman, S. H., Ali, A., Ghaleb, F. A., Rosman, A. S., &Marni, N. (2020). Database Forensic Investigation Process Models: A Review. IEEE Access, 8, 48477-48490. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9016047

[8] Jones, J., & Etzkorn, L. (2016, March). Analysis of digital forensics live system acquisition methods to achieve optimal evidence preservation. In SoutheastCon 2016 (pp. 1-6). IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7506709&casa_token=6R8Ce1YnpeIAAAAA:6XIOK-mh4hEFiCKkPvS6F7vz5Cnc4zDmi8bKatPI9eNXSlotTZY5b4dT79l5EG32SxuK0W3WUQU&tag=1

[9] Kaur, M., Kaur, N., Khurana, S. (2016). A Literature Review on Cyber Forensic and its Analysis tools. International Journal of Advanced Research in Computer and Communication Engineering, 5(1), 23-28.

[10] Fu, X., Gao, Y., Luo, B., Du, X., &Guizani, M. (2017). Security threats to Hadoop: Data leakage attacks and investigation. IEEE Network, 31(2), 67-71. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7827929&casa_token=VvqwjaViqYkAAAAA:DQ2j3v6B9KRiiuNAH8EdTJSMxsOzEuvVX9c2M5E2410_PyLcFcCZKb6VkNtenur0LM-sWt1qbjY

[11] Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and Big Heterogeneous Data: A Survey. Journal of Big Data, 2(1), 3. https://link.springer.com/article/10.1186/s40537-015-0013-4

[12] Javadianasl, Y., Manaf, A. A., & Zamani, M. (2017). A practical procedure for collecting more volatile information in live investigation of botnet attack. In Multimedia Forensics and Security (pp. 381-414). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-44270-9_17

[13] Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. In IFIP International Conference on Digital Forensics (pp. 17-36). Springer, Berlin, Heidelberg. https://link.springer.com/content/pdf/10.1007/978-3-642-04155-6_2.pdf

[14] Bellinger, G., Castro, D., & Mills, A. (2004). Data, information, knowledge, and wisdom. https://homepages.dcc.ufmg.br/~amendes/SistemasInformacaoTP/TextosBasicos/Data-Information-Knowledge.pdf

[15] Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–Challenges in supporting the organisational security function. Computers & Security, 31(5), 643-652. https://www.sciencedirect.com/science/article/pii/S0167404812000624?casa_token=tDzspb2LXloAAAAA:5PrH7ObP8JVUrjN7RZA1ocMYvF0QIfjkWRV2-4Q6l6noeVsPF7sfYCi1ZQ-H2fG3HL56kQz9zEY

[16] Watt, A. C., & Slay, J. (2015). First Responders Actions to cope with Volatile Digital Evidence. International Journal of Electronic Security and Digital Forensics, 7(4), 381. https://www.inderscienceonline.com/doi/abs/10.1504/IJESDF.2015.072182

[17] Ibrahim, N. M., Al-Nemrat, A., Jahankhani, H., & Bashroush, R. (2012). Sufficiency of Windows Event Log as Evidence in Digital Forensics. In Global Security, Safety and Sustainability & e- Democracy (pp. 253-262) Springer, Berlin, Heidelberg. https://repository.uel.ac.uk/download/2a0ad15d0574a2ebc4092dd59cfa017501a051f0d102b7ce8f76be817e43edd6/433298/Sufficiency%20of%20Windows%20Event%20log%20as%20Evidence%20in%20Digital%20Forensics2.pdf

[18] Mouhtaropoulos, A., Li, C. T., & Grobler, M. (2014). Digital forensic readiness: are we there yet. J. Int't Com. L. & Tech., 9, 173. https://heinonline.org/HOL/Page?handle=hein.journals/jcolate9&div=20&g_sent=1&casa_token=myk9ar5om1kAAAAA:gjGuq5t2tZjkJ0KoFQeTeb0OpR1xfCIxteukuDSXbMKFcLvPXoFp_vsHgmYzOzPCzpHk-uRddg&collection=journals

[19] Kothari, C. R., & Garg, G. (2016). Research methodology: methods and techniques. New Delhi, India: New Age International.

[20] Sahinoglu, M., Stockton, S., Morton, S., Barclay, R., & Eryilmaz, M. (2014). Assessing Digital Forensics risk: A metric survey approach. In Proceedings of the SDPS 2014 Malaysia, 19th International Conference on Transformative Science and Engineering, Business and Social Innovation. https://www.researchgate.net/profile/M_Sahinoglu/publication/268507819_ASSESSING_DIGITAL_FORENSICS_RISK_A_METRIC_SURVEY_APPROACH/links/546d4ad90cf26e95bc3cb0a0/ASSESSING-DIGITAL-FORENSICS-RISK-A-METRIC-SURVEY-APPROACH.pdf