Improving Distributed Forensics and Incident Response in Loosely Controlled Networked Environments

Irvin Homem, Theo Kanter and Rahim Rahmani

Stockholm University, Post Box 7003, 164 07, Kista, Sweden
{irvin*, kanter, rahim}@dsv.su.se

Abstract

Mobile devices and virtualized appliances in the Internet of Things can be end nodes on varying networks owned by different parties over time, while still seamlessly participating in licit or illicit activities. Digital Forensics and Incident Response (DFIR) tools today struggle to perform digital investigations in such loosely controlled networked environments as they face several challenges including: scarcity of resources, availability, trust, privacy, data volumes, velocity and variety. In this paper we analyze the state of research in DFIR in networked environments, identifying the challenges facing DFIR tools particularly in loosely controlled network environments. We present the requirements for a system to address these challenges at the various steps of the typical digital investigation methodology. From this we identify the need for support from Peer to Peer (P2P) overlays and discuss their relative merits and drawbacks in order to identify those that would best support DFIR in loosely controlled networked environments. Finally we incorporate both structured and unstructured P2P overlays in various capacities in our architecture in order to organize devices in loosely controlled networks, using context information, thus enabling efficient capture, analysis and reporting of artifacts of use in digital investigations.

Keywords: Digital Forensics, Incident Response, P2P Overlays, Open Distributed Systems, Uncontrolled Environment, Internet of Things.

1. Introduction

“Any networked organization is likely to suffer either sporadic or constant compromise”.[1] Today, it is a commonly accepted idea in security circles that security measures put in place to protect against, or reduce the effects of malicious activity, do eventually fail. Security breaches are inevitable. An integral way to react to their inevitability is to learn from them as they happen, or in the worst case, after they have come their completion. It is for this reason that Digital Forensics and Incident Response (DFIR) techniques have increasingly intermingled, and become critically important in the overall “security posture” of every organization, information system, or individual. This is because there is an aspect of learning and understanding of malicious activity that occurs in digital investigations, and is channeled into Incident Response mechanisms in order to effect an appropriate reaction. This is even more evident in dynamic environments such as those consisting of networked devices, particularly if they are not under the definitive control of an administrative unit and involve connectivity to public networks such as the Internet. Moreover, it is challenging to perform digital forensics and incident response techniques in such environments due to
this lack of full control, as a lack of full control implies a lack of trust in the environment, which is critical for a digital investigation.

1.1. Defining Loosely Controlled Networked Environments

Extending from the term used in [2], a loosely controlled networked environment is characterized by private devices belonging to users, making use of publicly available, shared network and computing infrastructure that are provided by a service provider. There is a trade-off between the users and the service providers on how much control either party has over participating devices and the services provided.[3] From the users’ perspective they own the devices, while the infrastructure is shared with others, but owned by the service provider. In such an environment, where there is a shared infrastructure, division of responsibilities and potentially different intentions, two main adversarial models can be considered, that is, the “Honest but Curious” adversary and the malicious adversary.[4, 5] The “Honest but Curious” adversary follows the designed protocol, however she goes further to pursue goals of self-interest that may contradict the system’s other participants goals. Service providers generally fall into this category as is explained later. The malicious adversary behaves arbitrarily and always attempts to break the prescribed protocol of a system. Any maliciously acting participant, be it the service provider, an external actor or any other user sharing the infrastructure, could be classified in this category.

Cloud infrastructures, mobile devices and ad hoc network installations inherently embody the accessibility of private appliances to public network and computing resources that are usually controlled by either known or unknown third party entities. Thus the term “Loosely-controlled” stems from this fact that there are a lot of user-end devices (appliances) that run off network and computing resources that are not entirely in their control.

1.2. Control in Cloud Infrastructures, Mobile Devices and Ad hoc installations

With mobile devices, the level of control that the user has of the cellular network that they use is rather limited. Baseband operations are highly restricted on mobile devices and are usually only accessible to the kernel of the mobile operating system and the SIM card. Operations from user space are generally not permitted. Even in terms of software development, baseband related applications are only developed by trusted manufacturer related entities and documentation is generally rather scarce. This could be a measure of security, however it is also a loss of control over connectivity capabilities of a mobile device. This means that users have to trust the manufacturer and the service provider that they will not undertake further activities contrary to the user’s objectives, as seen in the “Honest but curious” adversarial model, in using their privileged control over the baseband connectivity options. Profit-motivated objectives such as is seen in [2] can provide the impetus to service providers to act in this manner, thus diminishing the trust that the user has due to the loss of control of certain functionality of their devices.

Additionally, users are often accustomed to connecting their mobile devices to other networks such as Wi-Fi networks at home, at workplaces, at friends’ houses, or even at public places such as schools, restaurants and public transportation hubs. Mobile devices may also be connected to other non-standard forms of networks such as with Near Field Communication enabled devices. In many cases these networks are not
under the control of the mobile device owner and thus the activities occurring over the
network, whether licit or illicit, may not be under the control of the device owner.

In some cases it may be said that the service provider that maintains control over the
network is known by the user to a certain extent, such as in the case of Wi-Fi networks
at workplaces, restaurants and public transportation hubs. However, mobile devices
may also participate in ad hoc networks that may be Wi-Fi based (such as with gaming
devices) or Bluetooth based (such as Bluetooth personal area networks). Other small
scale embedded devices, of the Internet of Things type, may also participate in
spontaneously changing ad hoc networks. In such cases, there is more uncertainty as to
who controls the intermediate devices, the border gateway and onward connectivity to
the Internet.

With public cloud services there are varying levels of control of the appliances or
network connectivity that one has.[3] With Software as a Service (SaaS) offerings, such
as Gmail or Google Docs one only has control over the specific application
functionality and it’s settings as exposed to the user by the service operator. Platform as
a Service (PaaS) providers such as Heroku offer further capabilities such that the user
can control the configuration and running of certain applications, such as web servers
and development tools, however they cannot control actual host devices, operating
systems or networking capabilities to a great extent.[6] Infrastructure as a Service
(IaaS) operators such as Amazon Web Services, offer the most control in that the user
can customize and deploy a variety of machines, configure the operating system, the
applications, network topologies and other intermediate networking device capabilities
to a significant extent. However, in general all public cloud service resources are shared
among several users. In such multi-tenant infrastructures, an individual user does not
know exactly which other user is making use of the same physical hardware, or whether
they are malicious or benign, thus the infrastructure and the services provided cannot be
trusted entirely.[3]

In all the above cases it can be seen that though a user may make use of certain
resources, such as network or computing resources, they may not be in full control of
these resources. Furthermore, the users have no knowledge of which other devices are
sharing the same resources, or what other activities may be occurring on these shared
resources. This lack of full control or knowledge of the state of resources poses a
challenge to the users in that they must trust the service provider, the centrally
administered infrastructure provided and other participating users, despite the risk of an
“honest but curious” adversary or a malicious adversary. In such a case this is
problematic for undertaking forensic investigations in such an environment. It can be
seen that collecting evidence in a forensically sound manner, or undertaking forensic
analysis with such constraints is a difficult task due to the lack of control, and thus trust
in such an environment of shared and distributed resources and responsibilities.[7]

Even in the case of a known provider of such shared resources, trust must be placed
in the provider to ensure implementation of suitable security measures, as well as
appropriate monitoring and forensics capabilities being in place. However, placing full
trust in the service provider is generally not considered a good security strategy given
the “Honest but Curious” adversary model.[4][5] Many service providers are said to be
“Honest but Curious” that is, they provide customers with resources, but they can also
make use of the data that one puts onto their resources, usually as metadata, either to
improve their services or to be sold off to other willing buyers.
1.3. The Need for Independently Controlled DFIR Mechanisms

More critical, is the issue of security lapses among these provided services of computing, storage and interconnectivity. As a user of these services, one would expect security mechanisms to be put in place. Most serious vendors would provide these in the form of firewalls, intrusion detection systems and back-up, or fail-over mechanisms. However, users of these services may also want other more reactive mechanisms that could enable them to perform forensic activities [8] in order to understand malicious activity, prosecute culprits, or respond to security incidents dynamically and rapidly. Moreover, if the service provider is also deemed to secretly harbor malicious intent, then private users need to either have their own set of services to provide these digital forensics and incident response (DFIR) mechanisms, or have a means to enforce that a provider provides such either through law or contract.

In the scenarios described in the previous section, where the controller of the network is not specifically known and fully trusted, the best security strategy is to assume that their motives are adversarial, given the possibility of an “Honest but Curious” adversary or a malicious adversary as earlier described. Thus, a “defense in depth”[9] approach, whereby one implements their own security mechanisms in addition to those provided by the service provider, is the preferred alternative.

Further to this, there has recently been a significant increase in malicious activity perpetrated over networks through malware and the exploitation of vulnerabilities. Examples of these include Ghostnet [10], Operation Aurora [11], Stuxnet [12], Zeus [13], Duqu [14], Flame [15], Regin [16], and Dendroid [17]. It took a significant amount of time to discover these sophisticated malicious activities as they by-passed common preventive security measures implemented by the organizations or their service providers. The Mandiant M-Trends 2014 report [18] indicates that in 2013 it took on average 229 days (approx. 7.5 months) to discover a security breach. The Mandiant M-Trends 2013 Report [19] indicates that it is the analysis process (in the form of digital forensics, reverse engineering and code reviews) over several months or years, that has eventually exposed malicious activity, rather than traditional security mechanisms.

Individuals and organizations interested in the normal operation of their business processes using cloud infrastructures, or supported through mobile networks, are not yet able to detect sophisticated attacks.[18] They are not equipped with dedicated digital investigations personnel, or incident responders to analyze particular incidences of surreptitious malware.[20] The service providers are also usually more interested in the performance of their hardware and software with only some interest in implementing defensive security measures such as firewalls and intrusion detection systems. They are generally not yet capable of providing a full set of reactive security measures such as digital forensics and incident response on a large scale to all their customers. They may only do this in a generic fashion on their backend servers, if their infrastructure itself is affected. It is significantly more difficult to deal with an incident affecting client devices/ appliances affecting a large number of their customers – more so in a timely manner. Furthermore, these client devices/appliances are not always equipped with capabilities to understand and respond to attacks, particularly in cloud infrastructures and mobile devices which are usually directed at performing very specific tasks due to limited resource availability.

Redding[21] developed an architecture for providing DFIR procedures supported through a structured P2P overlay using JXTA within the controlled environment of an organization. It does not handle the trust, security and privacy concerns of a loosely
controlled network environment brought about in shared resources and conflicting
goals. Furthermore it makes use of a single structured P2P overlay that is not built for
resource constrained devices, high performance, network throughput or dealing with
large amounts of data – that are typically needed in loosely controlled network
environments. Thus, there is a need to find ways of providing these reactive services of
digital forensics and incident response directly to the customers for their constrained
devices/appliances within loosely controlled networked environments in an easy to use
manner – perhaps in an independent and automated fashion. This would empower the
individual entities such that they may be able to analyze, investigate and respond to
malicious activities on their own devices and networks (physical or virtual) to their own
contentment without the initial need for a centralized infrastructure or specialized
technical digital investigation expertise – that is in increasingly short supply in the
industry.

1.4. Contribution

The term “Loosely Controlled” networked environments has been described as being
categorized with private devices sharing public resources. This results in challenges
of trust, security, privacy and resource availability. We have identified that cloud
infrastructures and mobile devices exhibit this nature of being exposed to loosely
controlled network environments and further exhibit the presence of large amounts of
data. It has been seen that there is an increase in malicious activity and that current
preventive security measures are not as effective in discovering new sophisticated
malicious activity. More reactive approaches such as digital forensics and incident
response are needed, however they require a lot of infrastructure, computational
resources and technical expertise that service providers are not yet willing to invest in.

The alternative is to introduce automation and distribution directly among the
appliances in order to improve performance of the currently manual or semi-automated
tasks required of a digital investigative process. The challenge facing this option is that
most appliances that are involved in loosely controlled network environments are
largely limited in terms of resources. Furthermore, due to the lack of trust in the service
provider, combined with the inherent nature of such devices to shift across networks,
there is a need for an independent and collaborative means of performing a digital
investigation without relying fully on a third-party provided centralized infrastructure.

In this paper, we highlight the challenges facing digital forensics and incident
response in loosely controlled networked environments. We identify the need for a
trusted independent infrastructure to support the digital investigation process in such an
environment and posit that P2P overlays can assist in this. We outline the requirements
of such a P2P system for DFIR purposes, considering both structured and unstructured
P2P overlays. Finally, we propose improvements for the LEIA architecture [22] using
ideas from [23, 24, 25, 26, 27] and [28], that would enable the distribution of
information in such a network, thus enabling a more effective system for performing
digital forensics and incident response in a collaborative manner in loosely controlled
network environments.

1.5. Overview

The rest of this paper is organized as follows: In Section 2 we describe background
concepts and other studies related to digital forensics in networked environments and
peer to peer overlays. Section 3 focuses on identifying the challenges that face digital
forensics and incident response in loosely controlled networked environments. The various overlays and the challenges that they address at the different stages of the digital forensics process model are addressed in Section 4. In Section 5 we describe the architecture and the proposed enhancements that are needed to support digital forensics and incident response in loosely controlled environments. Finally in Section 6 and 7, we present our conclusions and outline future work, respectively.

2. Background and Related Work

In this section we briefly look into the various bodies of knowledge that encompass the focus of our study. We highlight the typical digital investigation workflow and how it is applied in networked environments. We also analyze key contributions in the developments of digital investigations in loosely controlled network environments such as those among cloud appliances and mobile devices. Research efforts regarding the management of information from incident investigations and P2P overlays in order to assist in enabling automation through tool interoperability and machine-to-machine communication are also discussed in this section.

2.1. Digital Forensics and Incident Response in Networked Environments

Digital investigations come into play when security measures fail to detect or prevent malicious activity. Digital investigations follow a prescribed workflow termed as the “Digital Forensics Process” model that involves identification and acquisition of evidence, analysis of the evidence, and reporting or remediation.[29] Incident Response is also sometimes included as part of the Digital Forensics process either as part of the initial stages of identification and collection of evidence, as part of the remediation process, or both.[30] This is specifically noted in digital investigations in networked environments where in many cases the malicious activity is persistent and continues while the investigation proceeds.[31] The importance of preparation for the eventuality of malicious activity occurring, the detection of its first signs from multiple sources, the subsequent forensic analysis and rapid response, are also emphasized in cases involving networked environments.[31] This done through implementing monitoring and data collection mechanisms at strategic points in the networked environment in order to detect malicious activity as early as possible as well as store data that can be analyzed further in a forensic manner. Rapid response is needed since malicious activity is usually discovered while it proceeds [31], and remediative actions such as blocking communications or killing communicating processes may be required to be effected as soon as possible in order to reduce possible damage.

As with “Big Data”, DFIR in networked environments faces the same challenges of “Volume, Velocity and Variety”. [32] Typical cases in networked environments involve several devices, generating, transmitting or storing several terabytes of data in varying heterogeneous formats in different locations. This has called for research into ways of tackling these problems which started with the development of distributed digital forensics architectures. [33] There have been several follow up developments in the form of tools as seen in [34, 35, 36, 37], evidence storage and exchange formats [38] [39] [40] [41] [42] and networks forensics architectures for large scale networks with rapid remote evidence acquisition, storage and processing at the focus as seen in [43] [44] [45] [46] [47]. All of these innovative ideas are premised on the grounds of a controlled network environment such as that in an enterprise. To the best of our knowledge, there has been only one study [22] that provides for DFIR architectures for
less controlled environments, encompassing the digital forensics process model. This study mainly makes use of 2 P2P overlays to enable automation of some parts of the digital forensics process model, but still relies on a centralized backend for data storage and analysis. We extend upon this by adding further decentralization of other phases of the digital forensics process model through harnessing the strengths of a variety of P2P overlays. We thus edge closer to enabling independent and automated digital investigations through the full decentralization of the digital forensics process model in loosely controlled network environments.

Nevertheless, specific efforts in the loosely controlled network environments space within DFIR in cloud environments and mobile devices have been made in recent years. The main focus has been to understand these relatively new potential digital crime scenes. To this effect, there have been several studies mapping out the areas such as [48] [49] [50] [51] [52] [53] [54] mapping out cloud environments; [55], [56] and [57] have discussed the challenges that DFIR faces in mobile environments.

While discerning these environments, efforts have also been made at trying to semi-automate the manual investigative techniques that are being developed. Detection, or identification of malicious activity has been a major focus, as malicious activity is a moving target and is always changing. This obliges researchers to continuously look into new detection methods. Notable efforts made here include [58] [59] [60] [61] [62] [63] [64]. Individual efforts on the semi-automation of collection of evidence and analysis have also been made such as [65] [66] [67] [68].

While previous research has identified the specific challenges facing DFIR in these environments, we focus on the challenges that would face an independent, automated distributed system that performs digital forensics and incident response in such loosely controlled networked environments. Furthermore, previous research has contributed to the progress of specific challenges in individual contributions towards identification, collection and analysis of specific artifacts of evidence of malicious activity in these environments. We bring these together in a unified distributed architecture that spans the entire digital forensics process model making use of the strengths of multiple P2P overlays in order to enable independent and automated digital investigations in such loosely controlled networked environments without relying on a centralized infrastructure that is under the control of a third-party.

2.2. Incident and Investigation Information Management and Exchange

In digital investigations that involve multiple sources of evidence, or several entities (devices, individuals or organizations), there is need to manage this information. There are several reasons for this. The main reason is to maintain the “chain of custody” and the forensic soundness of the evidentiary data being collected. Other prominent reasons in recent times include the need to handle large amounts of data, the need to distribute evidence data for analysis among larger teams, and the need to share information on the understanding of the latest threats or breaches that have been discovered in order to assist others, and the greater security community at large.

On the front of maintaining the chain of custody and forensic soundness, while also being able to distribute evidence to others to share analysis tasks there have been efforts such as [38] [40] [41] [42]. High level metadata about the evidence involved in the case and the investigators performing the analysis. Some metadata about artifacts within the evidence container are also maintained with the aim to allow for the same evidence storage container to be shared with other investigators who may plug the evidence into other tools to perform further analysis. The aim being to facilitate exchange of evidence
in order to enable distribution of forensic analysis tasks. This has allowed for semi-automation of the collection and some parts of the forensic analysis as is seen in the initial development of [69] [44] [45]. However these tasks are still largely dependent on human operators to confirm the identification of incidents and perform the analysis of the evidence. The improvements on [44], resulting in [46] could be argued to be closer to automating the triage process, thus enabling simple identification and initial analysis, however, similar to the others it is still reliant on being in a controlled environment and having a centralized evidence storage infrastructure.

Sharing information about malicious activities in order to inform other entities who might be able to react faster in detecting and understanding these threats has also seen some recent developments. The aim of this was to standardize the description of certain artifacts that indicate the occurrence of a certain security incident in order to facilitate automated detection, collection and analysis of such events. An initial IETF standard on the Incident Object Description Exchange Format (IODEF) [70] was proposed but not actively taken up. In recent times the Indicators of Compromise (IoC) standard [71] [72] [73] proposed by Mandiant has seen better uptake by the security community. There have also been other initiatives by the Mitre Corporation such as the Cyber Observable eXpression (CybOX) [74], Digital Forensic Analysis eXpression (DFAX) [75], Structured Threat Information eXpression (STIX) [76] and Trusted Automated eXchange of Indicator Information (TAXII). [77] These efforts work together in order to standardize threat information and digital forensics artifacts such that they can be shared among entities (devices, individuals and organizations) in a machine digestible format while still being human readable, thus enabling information exchange.

As proposed in the TAXII standard [77], there are three main models for sharing incident related information: A unidirectional centralized mode, a bi-directional centralized mode and a peer-to-peer mode. In this paper we draw upon the inspiration of the this peer-to-peer mode in order to develop an architecture for the sharing of incident information and digital forensics artifacts (threat intelligence information) in order to enable faster and more effective incident response. The peer-to-peer nature would enable the independent exchange of information and distribution of forensics artifacts without relying on a centralized infrastructure that may be under the control of the service provider. While the TAXII standard does not specify a particular P2P overlay we analyze several overlays in order to determine the most suitable ones.

2.3. Peer to Peer Architectures

Computer systems and network architectures that rely on a centralized infrastructure suffer from the major drawback of having a single point of failure. Most, if not all, digital forensics and incident response architectures, so far, rely on having a centralized incident information source, evidence storage location, or forensic analysis repository. Redding proposed a peer-to-peer system to perform the entire digital forensics process flow, but did not go into the particular P2P protocols enabling the infrastructure. Furthermore, this work was aimed at a controlled network environment within the confines of an organization. Pringle and Burgess [47] proposed a distributed storage platform (filesystem) with inherent assurances of integrity and provisions for performing forensic processing in a distributed manner. Though it allows for distributed storage and processing, the presented filesystem seems to be built for a controlled network environment as there is mention of administrative personnel and production grade servers in use as individual peers. In the loosely controlled network environment that we describe the devices involved, such as mobile devices and cloud appliances are
resource constrained by definition and need to be able to perform their DFIR tasks in an independent way - devoid of a centralized infrastructure or administrative control. To this effect we aim to do this using a Peer to Peer (P2P) architecture making use of a set of different overlays. This enables the delegation of what would have been server-side tasks to individual peer devices, such that they can act as both clients and servers depending on their circumstances. This could potentially spread the load and also remediate the problem of a single point of failure.

P2P overlays are generally categorized into three basic classes according to the logical architecture of the network of participating nodes that they create. These categories are: Structured overlays, Unstructured overlays and Hybrid overlays [78] [79] [80] [81]. Further to this, there are various flavours of these 3 general categories that attempt to make the individual overlays either tend towards being more centralized or more decentralized, for the sake of robustness of the network functionality based on the needs of the particular application area of the overlay. [79]

Structured overlays are termed as such due to the organized (structured) placement of resources (data or computational resources) and resource discovery information within the overlay network in an ordered manner. The idea behind this is to ensure that resources can always be found at a distinct location, thus making queries for these resources more efficient. The most common way of achieving this structured organization is through the use of Distributed Hash Tables (DHT’s), whereby hashing algorithms are used to create key-value pairs that represent the addressing information and the resource itself, respectively. In general a DHT is a large table of key-value pairs that is split into pieces and stored at different nodes participating in the overlay. The determination of the hashing algorithm used, and thus the “nearness” (distance) metric that determines the node where the specific key-value pair will reside is chosen according to the needs of the application. A simplistic example of this nearness could be the amount of similarity between the hash value of the node’s address and the key (the hash value) of a certain piece of data or resource address. Structured overlays attempt to ensure that there is uniform distribution of the load among the peers, however this may not always be the case. Overloading of certain parts of the overlay could occur [82] depending on the properties of the hashing algorithm and the data or resource addressing scheme used. Uniformly distributed hashing algorithms are preferably used to attempt to avoid this overloading, however it may still occur due to the characteristics of the Pigeonhole problem in hashing algorithms. It should be noted that this overloading may be intentional or unintentional, and is only problematic if it occurs unintentionally. Another drawback is the deterministic nature of the node discovery and resource placement that makes it easy to determine the location of an object and modify or replace it, thus causing security concerns particularly in terms of integrity and availability. [82] The main advantage of structured overlays is that they provide deterministic and usually more efficient look-up/ searching performance. Examples of well-known structured overlays include: Chord [82], Kademia [83] and Pastry [84].

Unstructured overlays revolve upon the idea that either their search/look-up process, or the nodes where resources are found stored at are non-deterministic. In terms of the look-up (peer discovery) process, it may be that the peer queries a specific centralized registry service, or that it uses bounded flooding techniques (E.g. Time-To-Live - TTL values, or time-bound gossiping) to find a node. The resource placement/ locations in unstructured overlays are always random. Due to this randomness in locating resources, redundancy of data /resources is a necessary and beneficial requirement that enhances the reliability of unstructured overlays. The randomness and redundancy in turn also
contribute to the security of the system in terms of integrity and availability in that they make it a little more difficult to determine the exact location of a resource in order to maliciously modify it. The main drawback of unstructured overlays is the possibility of flooding the network with query messages for difficult to find resource objects. The combination of the use of TTL’s and redundancy usually prevents this. Examples of well-known unstructured overlays include: Gnutella [85], BitTorrent [86], Cyclon [24] and FastTrack (Kazaa).

Hybrid overlays are said to make use of both structured and unstructured overlay paradigms for different aspects of their functionality. In most cases the search/look-up (node discovery) process is that which follows a structured overlay paradigm, while the resource placement follows an unstructured mode of operation. In this way search performance improves due to the use of structured overlays and availability is achieved through redundancy in the unstructured overlay paradigm. Well known examples that follow this unstructured and structured overlay combination include Structella [87] and Kelips [88]. Hierarchical overlays, such as the proprietary Skype protocol, are also sometimes considered as a particular form of hybrid overlay, in that they make use of multiple tiers of often different overlay paradigms in an attempt to organize the network in a particular manner. Not much is known of the Skype protocol, however it is known to have a layer of distributed super-peers to ensure availability and robustness of the overall network.

Traditionally, P2P overlays have been built to support distributed messaging, file sharing and computation. [89] When considering the suitability of specific P2P overlays for performing particular tasks, several key elements related to the routing and reliability of the system need to be taken into account [79] [81] [89]. Some of these key elements include: Node Interaction Frameworks, Peer Discovery, Overlay Maintenance, Resource Placement and Look-up, Network Resilience, Security and specific overlay functionality. These elements are described below:

i. Node Interaction Framework: Depending on the functionality required of the system, a centralized, unstructured, structured or hybrid means of interaction may be utilized. Commonly used interaction frameworks include: Centralized registration, Distributed Hash Table (DHT) based addressing, Publish-Subscribe dissemination, Flooding and Epidemic dissemination.

ii. Peer Discovery: This is the process of identifying other nodes in the overlay. It is usually a process done when a node intends to communicate with another node, join an overlay, or at the initial commencement procedures of an overlay network when attempting to find other peers to join.

iii. Overlay Maintenance: This is the process whereby a network overlay accepts the joining of a new node, or deals with the consequences of the departure of a node from the overlay. The admission procedure entails the registration and addressing of a node as well as assigning it tasks, while the departure procedure deals with the deregistration and notification to others of the node’s departure, as well as reassignment of the tasks that the departing node previously held.

iv. Resource Placement and Lookup: This entails the registration, addressing of particular resources that are to be designated, or found at particular nodes. It also involves the searching process with the aim of locating a particular resource.

v. Network Resilience: This is the ability of the network to withstand high levels of churn, that is the joining and departure of large numbers of nodes at rapid rates.
This usually seen as an issue of availability and scalability of the overlay’s service being provided. It is usually facilitated through redundancy, load balancing and fault tolerance recovery mechanisms in order to maintain reasonable levels of performance without noticeable degradation.

vi. Security: This is the capability of a system to be able to maintain control over its operations such that it is not susceptible to performing in an unexpected manner. This is usually attained through achieving confidentiality, integrity, authentication, authorization, accountability and non-repudiation according to the system’s needs.

vii. Specific Overlay Functionality: This is the most important element in determining the suitability of an overlay. This is because the specific required functionality dictates the extent of the choices of all the other core elements described above.

P2P overlay networks in general need to perform message exchange in order to facilitate the aforementioned key elements. In particular, they often need to perform message exchange in order achieve the Specific Overlay Functionality. Some of the commonly seen functionality include: information dissemination, aggregation of data, data streaming, file-sharing, text searching, network optimization and delegated processing.

In order to achieve this specific functionality, which in the case at hand is to perform digital investigations in an independent and automated manner, further information needs to be shared and exchanged, other than node and resource addressing information. This extra data that is to be collected and shared is usually termed as context information.[27] This is usually used to inform the overlay network on how it should organize or reorganize itself in a more efficient manner to facilitate the required specific functionality. In our case this specific functionality is to enable the independent automation of the phases of the digital forensics process model. More specifically: evidence triage phase, evidence acquisition and storage, analysis, documentation and remediation. The distribution of this context information with DHT-based structured overlays as the underlying platform has been addressed with DCXP [26, 27] and the KBR API [90]. We make use of these ideas of sharing context information and combine the strengths of various other structured, unstructured and hybrid P2P overlays in order to apply them for specific uses to enhance our digital forensics and incident response system [22] that previously maintained a centralized backend. In this way we organize the underlying network in a more efficient manner to support further decentralization and automation of the digital investigation process within loosely controlled networked environments.

3. Requirements and Challenges

Performing digital investigations in loosely controlled networked environments with the aim of achieving automation and independence from a centralized, or otherwise third-party controlled infrastructure faces certain requirements and challenges. These can be categorized into 3 main groups: Those related to the actual digital forensics and incident response requirements; the concerns around the security of the forensics process in a loosely controlled environment; and the challenges brought about through using distributed systems to tackle the large amounts of data that are typical of loosely controlled networked environments. Some initial ideas on the challenges have been identified in [29] and [21], however they are largely aimed at networked environments within the full administrative control of an enterprise.
3.1. Digital Forensics and Incident Response Functionality

The phases of the digital forensics process model [30] are necessary functionality of any system tasked to perform digital investigations. In this section we describe the details of each individual phase. Redding’s architecture[21] is also based on the digital forensics process model, however the triage phase [57] was not dealt and the evidence collection, analysis and reporting were limited to network based evidence sources. We thus review the phases of the digital forensics process model, as described below in order to cater for multiple evidence sources as are commonly found in loosely controlled networked environments.

- **Triage and identification of potential evidence sources**: This capability revolves around the ability to rapidly discern the available sources of potential evidence sources (e.g. disk, memory or network) and if possible isolate the particular logical objects within these evidence sources that could be indicative of evidence of the activity being purported.

- **Acquisition of digital evidence**: This involves the collection of an evidence source in a complete, accurate and forensic sound manner. In certain cases completeness may not be possible, however it should be shown that the collection process procured as much as possible of the evidence source. Additionally it should be shown that the process did not significantly modify the resultant copy in as much as making the evidence not admissible in a court of law. Furthermore, future checks on the forensic soundness of the acquired evidence source should be made possible. This is usually done through the use of hashing techniques performed on the evidence data as it is collected. Provision for the extensibility of the acquisition capabilities should be present as new methods of acquisition are developed, or new sources of evidence may be discovered.

- **Analysis of the different evidence pieces collected**: The functionality here would involve the parsing of the different data sources in order to extract information; reduction of data in order to exclude that which can be confidently understood as excess (such as with “known system files”); correlation with external databases as well as correlation across acquired evidence sets; reverse engineering of malicious code or network traffic; recovery of keys, passwords and breaking cryptography. The components handling the analytical capabilities should be extensible as new methods of analyzing data are still being developed.

- **Provision for reporting on the outcomes of the entire process**: This is a key component of the overall digital investigation process and should be incorporated at all stages of the process within the system (Triage, Acquisition, Analysis and Remediation, Recovery, or recourse to legal proceedings).

- **Remediation, or further collection of evidence**: This functionality involves the actions that are taken after some understanding of the purported malicious event is gained. It may involve thwarting the malicious activity through blocking ports, deleting of files, killing of processes or modifying configuration files, among other procedures. It may also involve recovery mechanisms such as the restoration of data from backups. In certain cases, further triage and collection of evidence may be required in order to gain deeper insight into the malicious events in order to the advance the investigation.
It should be noted that these elements of the standard digital forensics process model are not necessarily sequential in nature. In some circumstances it may require that they occur in parallel and iteratively.

3.2. Security Considerations Around the Digital Forensics Process

For any system, and in particular a system charged with the responsibility of performing digital investigation related activities, the security of the system is important. Security is based on the trust that can be placed in the system to perform as is intended. Further to this, digital forensics has specific obligations that call for the need of the information being dealt with in a digital investigation to be trustworthy. This is because the data is eventually used to attribute malicious activity to the responsible actors and could result in criminal justice repercussions including fines, imprisonment or other similar punishments. It is imperative that the integrity of the data is trusted as it may determine whether punishment is rightfully meted to the culprit or wrongfully to an innocent party. In Redding’s architecture [21] security and thus trust is provided among peers in a controlled environment through the use of a centralized Public Key Infrastructure. In a loosely controlled network environment, as it has been shown earlier, the users would not want to trust a centralized infrastructure provided by a third party due to the possibility of them being an “honest but curious” adversary. In this section we consider the elements that are needed to achieve the necessary state of trustworthiness in a distributed system tasked to perform digital investigations in a loosely controlled network environment. It should be noted that both the system itself and the data it interacts with need to be considered.

The trustworthiness of the system impacts the trustworthiness of the data. The following are properties of the system that would contribute towards ensuring trust:

- **Integrity** of the system performing the collection, storage or analysis of the data. This means that data collected should be remain unmodified from the time it is acquired from the source, throughout the rest of the digital investigation process. Care should be taken that the means of acquisition is not compromised such that the data collected is manipulated while undergoing the acquisition process.

- **Accuracy** and **reliability** of analysis procedures implemented in the system. In order to be able to trust the results of a system performing the analysis in a digital investigation, the methods need to be accurate and reliable. This means that the methods used should be replicable in a scientific manner giving results that are acceptable by experts of the domain area, as is required of the Daubert Standard.

- **Authentication, authorization, accountability and non-repudiation** are necessary in order to ensure the chain of custody is maintained and can be traced.

- **Privacy or Confidentiality** enforcement by the system on the data that is being collected, stored and analyzed. This is perhaps the greatest concern for such a system with respect to its uptake among users. This is because the devices that commonly make use of loosely controlled networked environments are private devices. Such devices are often filled with large amounts personally identifiable or company data that is considered confidential, and if found in the wrong hands could be detrimental to the owners of the devices or the actual data. A compromise must be reached in order to maintain the secrecy and anonymity of such data while also allowing for evidence linked to malicious activity to be made available for the
due process of the prosecution of perpetrators to be accomplished. Unauthorized access to the data within the system should be prevented.

The trustworthiness of the potentially evidentiary data collected itself also plays a major role. Though this is not particular to loosely connected network environments it is well worth noting its importance in the realm of digital investigation. The trustworthiness of the data in itself relies on its completeness and its integrity.

- **Completeness** is considered synonymous with integrity of the data, however in digital investigations today it is often next to impossible to ensure that all the potential evidentiary information has been collected. In loosely controlled environments the fact that devices may change networks, or disappear off the network all together could affect the completeness of evidence collection. For example in a cloud environment if an appliance instance is terminated and re-initialized in a different cluster certain evidence may be lost. As completeness may be difficult to achieve, the correct identification and collection of data that is most likely to be useful to the investigation may be an alternate strategy to this tackling this issue. Another strategy may be to ensure availability through the replication of data among peers to ensure that forensic acquisition may be completed despite the disappearance of a device.

- **Data Integrity** is usually maintained through the maintenance of hash values held in a secure manner. Potential evidentiary data is usually hashed as it is collected in order to ensure that it is maintained as is, and any modifications to it can be detected through the mismatch of any future hashes procured.

### 3.3. Distributed Systems and “Big Data” Concerns

As described earlier in loosely controlled network environments there is a lack of trust in a centralized or third party entity to provide digital forensics services, thus there is a need for an independent and automated means of providing these services. However, loosely controlled network environments are also prone to having large amounts of data being transmitted, processed or stored among a variety of resource constrained devices. Digital investigations today in such environments also have to deal with these same large amounts of data being created, transmitted or stored among these heterogeneous devices.[33] The architecture in [22] proposed a centrally controlled scalable distributed filesystem as a backend for capturing and processing large amounts of digital evidence from devices in a loosely controlled network environment. Thus, we need to consider the factors that would play a part in achieving a further distributed system that can provide digital investigation services among large amounts of data and devices in an independent and automated manner devoid of a centrally controlled infrastructure. The facts that we consider are described below:

- **Independent infrastructure and Self Organization**: Due to the nature of loosely controlled networked environments, there is no trust in any particular centralized controlled coordinator or owner of the network. This results in the need for the individual participating peer nodes to be able to organize themselves in such a way that they can perform the required digital forensics and incident response procedures as much as possible without necessarily having a centralized infrastructure.

- **Availability**: In loosely controlled networked environments, network connectivity may be erratic as devices switch between networks or are terminated and reinitialized elsewhere. This means that the availability of certain services could suffer if a device suddenly is
unreachable. Thus, particular responsibilities should not be vested in individual devices. Redundancy is necessary in order to ensure that services are not unnecessarily interrupted.

- **Scalability**: Loosely controlled networked environments may not be bounded by the number of devices that are participating in the service. Thus a DFIR system focusing on such environment should be able to scale upwards or downwards, in terms of the number of devices, without a significantly noticeable degradation of performance.

- **Universality**: Due the lack of standardization and presence of proprietary formats, many devices that may be present in a loosely controlled environment today may be of widely varying specifications. This may be in terms of hardware capabilities, resources available, Operating System in use, file systems used, applications present or networking protocols used. Thus, a DFIR system for such an environment should be able to cope with such varied heterogeneity and be able to function normally.

- **Responsiveness**: In order to effectively perform in a decentralized environment, participating devices in such a system need to be able communicate with each other in order to maintain the organized structure of the overlay in the event of new nodes joining and others leaving. Such a decentralized system also needs to be able to rapidly react to the violation of security policies and communicate via message exchange schemes to notify other participating devices in order to ensure that the required DFIR procedures are initialized appropriately and proceed as expected at the affected nodes.

4. **Peer to Peer Overlay Considerations for Supporting DFIR**

As previously discussed, the standard DFIR process model is generally composed of 5 phases (Triage, Acquisition, Analysis, Reporting and Remediation). In this section we discuss the goals of these phases and how certain P2P overlays may be able to assist in achieving and independent and automated architecture for providing digital investigation services in loosely controlled networked environments. Within the scope of the different phases of the digital forensic process, we take into consideration several of the requirements described in the previous section, such as: achieving an independent infrastructure, availability, scalability, dealing with large amounts of data, privacy and security.

4.1. **Triage and Evidence Identification**

Triage involves the identification of the most indicative and beneficial sources of evidence in an attempt to reduce the amount of potential evidentiary information that is to be acquired. In certain cases this may involve performing live text searches on live running disks or memory in incident response activities on multiple machines in parallel as seen in [46] in order to identify particular devices for full acquisition and further analysis. It may also involve the comparison of hashes of files within a potential source of evidence against file hashes of known files. This common in trying to remove well known system files from disk-based evidence.

In order to perform triage activities that involve text searching, or querying for specific types of data, we posit that the use of structured overlays, particularly making use of distributed hash tables could assist in this process. This is because DHT-based overlays are
said to provide deterministic search times in the order of $O(\log n)$. This could prove to be beneficial in providing the ability to search over a decentralized network such as is the case.

For triage to be successful, replication of the data to be searched is also necessary for availability through redundancy, in case a certain node goes offline. This replication of data sources such as disk data, memory or network traffic can be resource intensive and thus rather difficult to achieve. Two methods are proposed here: *Piecewise replication*, whereby entire evidence sources are split into smaller chunks (pieces) and individually replicated across several devices; the other strategy is *Metadata replication* whereby detailed core characteristics of the evidence data sources are maintained at each data source as well as being replicated across multiple devices. It is yet to be tested whether either of these methods, or both in tandem could prove successful.

In order to achieve this replication, either structured or unstructured overlays may be used. Unstructured overlays (such as BitTorrent and gossip based algorithms) are more commonly inherently built with replication capabilities, however DHT-based structured overlays may also be used. In the case of structured overlays the choice of where the replicas are stored needs to be decided, while in unstructured overlays it is usually rather a matter of random placement.

As identified in [27], DHT’s may suffer from scalability and reliability issues in networks where there is a high amount of churn. In such cases the main suggested approach is to introduce a flavour of a centralized infrastructure through the use of some “super peers”. These super peers are to be nodes that are better endowed with resources as well as having more stable network connectivity in order to buttress the overall network. On the other hand, unstructured overlays, particularly those making use of gossiping protocols are generally built to be able to withstand networks with high amounts of churn and are known to produce eventual convergence of data.[25][91]

### 4.2. Evidence Acquisition

The aim of this phase is to obtain as much evidentiary data (disk, memory, network traffic, or logical abstractions of these) as possible, as fast as possible from a digital crime scene in a forensically sound manner and to maintain this forensic soundness throughout the chain of custody. Forensic soundness of the acquisition has traditionally been achieved by making use of tools that can be scientifically proven not to modify the data source while performing a low-level copy of the data. That is, the method used to perform the copy can be replicated showing the same results and that this means of copying is accepted by the domain experts and the scientific body in the domain of concern. This ensconces a level of trust that is required of the tools and techniques used in the digital forensics process. In addition to this, the integrity of the collected evidence is proven not to have been modified subsequently, through obtaining a hash value for the data as it is collected. This allows for the chain of custody to be maintained as the evidence data can be passed through the prescribed hash function later in order to ascertain whether it has been modified or not.

In live and highly dynamic networked environments where rapid incident response is required [31] it is sometimes not entirely possible to ensure that the evidence source has not been modified. [92][93] In such cases, which are becoming more common, care must be taken to ensure that as little as possible is modified and that all procedures undertaken are thoroughly documented. This is commonly experienced with the acquisition of live memory, live mission critical production systems that cannot be taken offline, and with mobile devices.
In any networked environment and in particularly a loosely connected one, it is of essence that acquisition be performed as rapidly as possible and that the evidence data is made available in a redundant form should any given node depart from the network. In addition to this the evidence data should also be made available in a form that can be used in the subsequent analysis phase, preferably in a form that is machine digestible and also possibly human readable.

As acquisition and subsequent storage of the evidence data is to be performed over networks and necessarily requires speed, an unstructured overlay such as the BitTorrent protocol is a likely front-runner candidate. This is because it is a greedy algorithm that ensures that transmission of data occurs in multiple streams and at the highest bandwidth available. Additionally, it offers high availability through the replication of pieces, particularly favouring the pieces that are less commonly available thus improving the availability of the data on the overlay. Further to this, the BitTorrent protocol performs hashing of the pieces of data that it distributes for integrity which would provide benefits for an environment that routinely makes use of hashes of data such as is seen in digital forensics.

BitTorrent draws part of its stability of peers being able to discover pieces of data distributed across the network through the use of trackers. Trackers are more stable peers that keep track of which peers contain which pieces of files. This is oriented towards being a more centralized infrastructure, though there are always multiple trackers. There is a possibility of a single point of failure here as there are usually not too many trackers in a BitTorrent network, thus a solution to mitigate this potential problem could be either to increase the number of trackers, or to distribute the tracker capabilities within a structured overlay such as those making use of distributed hash tables (DHT’s). This could provide a more stable tracker overlay such that peer discovery may be distributed but still providing a reasonably fast look-up process. As trackers are usually not found in extremely large orders of magnitude such a structured overlay may be a suitable modification to the standard BitTorrent protocol.

Other unstructured overlays making use of gossiping protocols may also play a role here in ensuring that the discovery of evidence data stored at a peer is more of a random process rather than a deterministic one. The motivation for this being to make it more difficult for an attacker to determine where the evidence is stored in the case that they are attempting to purge any evidence of their presence, as is common.

As discussed in the previous section, the acquisition and transmission of large sizes of evidence data (such as with disk and memory dumps) may introduce a bottle-neck and thus metadata may be collected instead of the actual full evidence source. The acceptability of metadata in judicial proceedings is still under discussion, however in an enterprise scenario where rapid incident response and remediation depends on the analysis of data (or metadata), it may be more prudent to make use of the metadata as it can be acquired faster.

4.3. Analysis

Current analysis processes include indexing of data for searching purposes, parsing data structures, correlating data from multiple data sources, creating timelines of events, analyzing communication patterns, analyzing malware capabilities, reverse engineering and attempting to break cryptographic protocols. To a large extent these procedures are highly manual and at best only parts of them have been semi-automated. To this end, it is difficult to suggest a particular form of P2P overlay that may assist in performing these tasks. However, it should be noted that for many of these tasks large
amounts of computing power are needed, thus strategies related to processing large amounts of heterogeneous data would be beneficial for this phase. “Big Data” processing frameworks such as MapReduce, Apache Spark and graph processing techniques could be used to assist some of these tasks through pattern matching and machine learning.

Mobilizing large amounts of computing power for a specific task in a loosely connected network environment may be difficult, however it may be possible to use a peer to peer overlay to share information thus identifying peers that are better endowed with resources. Distributed processing tasks may then be assigned to these better endowed peers. In order to achieve this sharing of information of stability parameters of peers, either a structured overlay, or an unstructured overlay may be used. A structured overlay may be motivated for privacy reasons such that particular data is only sent to and processed by a particular set of known identifiable peers that are within the DHT that is constantly cross-referenced. On the other hand, unstructured overlays such as those based on gossiping may be preferred due to the wider extent that gossiping can reach such that there is a greater likelihood of discovering some peers that might be significantly better endowed with resources. A hierarchical type of overlay making use of both categories could also be an option in order to achieve the best from both sides. In addition to this, a dedicated set of super-peers may also be introduced in order to enhance the stability, scalability and availability of the network. This also ties in well with the idea of having a hierarchical overlay in the same vein as the proprietary Skype protocol.

4.4. Reporting

This phase is highly tied to the previous phases and it is difficult to identify how a particular P2P overlay may assist with task. Hypothetically, documentation related tasks may be carried out with the help of a structured overlay in such a way that results of the previous phases are maintained as part of the data that can be reached through the addressing system of key-value pairs in a DHT. This could make it easier to search for documented facts in a similar way to text searching may be enhanced in the triage phase through the use of a structured overlay. The actual documentation tasks of producing a report is difficult to justify the need of a specific P2P overlay to assist its automation in a within a loosely connected networked environment. This is because it is more of a manual, human driven task that results as a by-product of all the other tasks.

4.5. Remediation

Practically this phase involves the updating of firewall rules, blocking ports on host systems, forcefully killing certain processes, quarantining certain executable files, modifying certain configuration files, isolating certain devices, changing user privileges, locking out certain users or even initiating the acquisition process of another set of evidence sources. The outcome is usually specific and directed towards a specific known entity or group of entities. This could include an identifiable device, or a logical entity on a computer system such as a configuration file, a port, a user or user group.

As these remediating actions are usually specific and directed, we posit that a “Publish-Subscribe” (pub-sub) form of overlay may be able to facilitate this directed information flow of actions to be performed without the need for a dedicated centralized source of information. Devices that are involved in the malicious activity could be automatically subscribed to push notifications from the set of peers that
perform the analysis activities. The pub-sub type of overlay can be supported by an underlying structured overlay (such as Scribe [94]), an unstructured overlay (such as Tera [95]), or building its own entire overlay (such as SpiderCast [28]) in order to support the dissemination of messages to the required destinations.

In a loosely controlled network environment where security and privacy are key concerns a pub-sub overlay must consider whether the routing of messages to the intended destination will require routing through uninterested peers, or even worse malicious peers. For this reason it is imperative that cryptography is used to hide the message and to ensure the integrity of the message being disseminated. In this sense, a public key infrastructure, or a PGP-based infrastructure could help in ensuring such cryptographic mechanisms are in place. In addition to this, for security reasons, redundancy of the message should also be considered, that is, the message should be sent through multiple routes such that there is a higher likelihood that the message gets to the intended recipient and is not maliciously dropped on the way.

5. An Architecture for DFIR in Loosely Controlled Environments

In this section we describe the architecture of a system intended to perform digital forensics and incident response activities in loosely controlled networked environments. The system architecture is based on the functional needs and requirements as identified and discussed in previous sections of this study. The main focus is directed towards the use of various P2P overlays within the system, while also making reference to prior work of the LEIA architecture [22], as well as incorporating the use of the DCXP protocol [26][27] to manage the information distributed by the structured overlays.

The architecture itself is based on the 4-tiered architecture of Live Evidence Information Aggregator (LEIA) that was built for remote evidence acquisition and processing. The use of P2P overlays was proposed in this prior study, mainly focusing on the use of gossiping protocols and the BitTorrent protocol in the evidence acquisition phase in order to improve the speed of the acquisition process and thus overall digital investigation process. In this study we extend this to add further uses of P2P overlays for a variety of purposes within the digital investigation process that could be particularly useful in loosely controlled networked environments. Table 1 summarizes the propositions and challenges addressed, with further explanatory details in the Section 5.2:

Table 1. Proposed P2P Overlays and Challenges Addressed

<table>
<thead>
<tr>
<th>Propositions</th>
<th>Challenges addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structured overlays in the Triage phase, and in supporting trackers for the BitTorrent protocol in the Acquisition phase.</td>
<td>Independent infrastructure, Availability, Scalability, Responsiveness</td>
</tr>
<tr>
<td>A hierarchical overlay consisting of both DHT-based overlays and gossiping protocols to facilitate identification of better endowed peers to be used in the Analysis phase;</td>
<td>Independent infrastructure, Availability. Scalability, dealing with large amounts of data</td>
</tr>
<tr>
<td>Structured overlays making use of DHTs for maintaining a searchable index of facts identified in the analysis phase such that they can be used for reporting purposes.</td>
<td>Independent infrastructure, Availability, Scalability</td>
</tr>
</tbody>
</table>
A Publish-Subscribe based overlay to facilitate the transmission of the remediation actions to the concerned nodes. | Responsiveness, Privacy

5.1. The LEIA Architecture

In order to explain the adjustments that equip this architecture for loosely controlled networked environments we briefly explain the original below. The architecture is made up of 4-tiers as explained below and as shown in Figure 1.

- **The Host-based Hypervisor system (HbH):** This is a privileged virtual machine monitoring layer between the physical system resources and the software performing the operational activities of the devices. It is intended to be the first point of detection of malicious activity through the use of an embedded IDS, as well as the initial point at which potential evidentiary information is acquired from the actual source, such as, disk drives, RAM memory and network interface cards. The evidence is to be collected and stored in a universally accepted format such as AFF4. As hypervisors are built to interact with physical devices from a lower more privileged layer of the system, they are a suitable source of evidence acquisition from a more trusted source. The use of Virtual Machine Introspection to facilitate evidence acquisition also goes to show their suitability. Additionally, they are known to have a smaller footprint, thus reducing the area of attack and improving the security of the system.

- **The Peer-to-Peer Distribution Architecture (P2P-da):** This is a combination of unstructured overlays making use of gossiping protocols and an adaptation of the BitTorrent protocol. The gossiping protocols facilitate the collection and dissemination of metadata sourced at individual nodes in order to determine if malicious activity is occurring, as well as to initiate the forensic acquisition process. The gossiping protocols also enable sharing of the utility metrics among the individual peers in order to organize the network in a hierarchical manner to facilitate transmission to peers with better resource capabilities. The adaptation of the BitTorrent protocol is used to ensure that acquisition is performed as rapidly as possible over the network, directing the acquired data to a distributed storage cluster termed as the Cloud based back-end. Availability of this data is enhanced through the replication afforded through both the gossiping protocol design and the inherent replication in the BitTorrent protocol.

- **The Cloud-based Back-end (CBB):** This is a centralized, but distributed large scale data store adapted from the Hadoop Distributed FileSystem (HDFS). The aim of this subsystem is to enable large scale data processing on potentially evidentiary data collected from various heterogeneous sources. The forms of processing discussed previously involve known file filtering, pattern matching and correlation of evidence from multiple sources. Due to its distributed nature and inbuilt replication capabilities it enables flexibility, scalability and availability.

- **The Law-Enforcement Controller (CBB):** This subsystem provides the interface for law enforcement personnel to perform complex queries in order to gather information related to ongoing investigations. The queries are aimed at improving the analysis procedures through determining specific information that may be sought after such as the events on other evidence sources that occurred before a known event, or the parties communicating with a known suspected party. The query language is intended to be based on SPARQL as the original uniform evidence format was described to make use of the Resource
Description Format (RDF) and the Web Ontology Language (OWL) to correlate events from multiple evidence sources.

The LEIA architecture was built for to automate the evidence collection and analysis procedures as well as to improve the overall digital investigation speed. It is aimed at an environment that is devoid of an administrative controller of the systems, however it still makes use of a centralized infrastructure in order to store and process the potential evidentiary information. In the following section we discuss improvements to the LEIA architecture in order to introduce further functionality for digital investigations supported by P2P overlays. These enhancements also improve the independence of the overall infrastructure in a loosely controlled networked environment, while still maintaining the digital forensics and incident response aims.

5.2. Support for Loosely Controlled Networked Environments

We incorporate a variety of P2P overlays in order to attain a more stable independent and automated digital forensics and incident response system for loosely controlled network environments. In the following sub-sections we describe some of the functionality of these proposed P2P overlays as well as the capabilities that they improve and challenges they address.

5.2.1. Enhancements to Support Triage

The use of a structured overlay that makes use of DHT’s is proposed here in order to make use of the search performance of DHTs. Triage requires quick searching and identification of potential evidence.

Assuming the use of a structured overlay such as the Chord [82] overlay, identifiers of data items would be hashed and placed at the node whose hashed identifier is close to, but less than that of the data item. The node where the data is stored and the preceding node are notified of the presence of the new data item, and their respective hash tables are updated. Data is replicated for the sake of availability at 2 other nodes. This is done by incrementing the data item identifier by 1 and performing a hash on this value, thus the 3 copies of the same data get 3 different identifiers and thus 3 different
pseudo-random locations within the overlay. This is done in a similar fashion as is seen in the DCXP protocol over the Chord overlay.

For the purposes of triage, metadata of events and objects are collected by the HbH peers in the form of CybOX [74] elements. (CybOX notation is chosen to facilitate machine digestibility in the analysis phase). These pieces of CybOX metadata are given identifiers. These identifiers are hashed and stored within the Chord DHT at their designated node. The individual metadata is replicated and transmitted along to the peers where the replicated hash-identifier will be stored. In this way the metadata can be sourced first hand through the DHT and if it fails to find this particular node, the replica can be found in one hop as the replicated data will be found on the node containing the and the “replica identifier”. In this way metadata is distributed around the overlay and searching can be performed in the same way that data look-ups are performed, and availability is improved through replication.

5.2.2. Enhancements to distribute the BitTorrent Trackers

In a file-sharing scenario using the BitTorrent protocol, the work of the trackers is to keep track of which peers have possession of which files, and thus which pieces of a file. The trackers act as a centralized directory service in order to find the relevant peers. There are usually a small fixed number of independent trackers that keep track of an individual file. As the BitTorrent protocol used in the LEIA architecture is based on the same tracker characteristics and functionality, it could be prone to being a single point of failure, particularly if the trackers are few. Furthermore centralized trackers would pose a problem of scalability should the need arise to expand the network.

An improvement to this would be to distribute the tracker service into a structured overlay making use of distributed hash tables (such as Chord). This could be done through storing the hashed identifier of the evidence data pieces, or files as the key, and the hash of the actual location of the file as the value. Similarly, availability of the service can be achieved through the replication of this key-value pair at multiple locations, as is described in the previous section with triage related metadata using the strategy in the DCXP protocol. If a node leaves the overlay a replica is made from one of the available copies in order to maintain a fixed number of replicas always available.

5.2.3. Enhancements for Distributed Processing for Evidence Analysis

The main need for the analysis process is the provision of large amounts of computational power. This may be achieved by organizing the network in such a hierarchical manner such that nodes with less computational power can transmit and store their evidence data items for processing at these nodes. The LEIA architecture previously provided for this sharing of information of utility metrics through epidemic (gossiping) protocols thus ensuring that utility metrics are widely shared. Once the hierarchical topology is achieved, the addressing and discovery of suitable more stable nodes could be achieved through a DHT based addressing scheme. In this way epidemic protocols such as Cyclon [24] can work together to update the DHT’s with the values of the addressing information, while the look-up process to determine where the set of peers where the data can be sent for processing can be possibly done with fewer hops than with a gossiping protocol. The actual transmission of the data would be done using the BitTorrent protocol whereby the torrent file (or the reflection as in the LEIA terminology) is forwarded to the more stable peer (or set of peers) which can then
request from the DHT for the locations of the individual pieces. In effect this produces a form of hierarchical overlay that makes use of 3 different overlays. In addition to this, super-peers that are built to be stable, may be added to the network in order to ensure that there are always more stable peers. This could be argued to be a drawback - adding a controlled entity within the environment - however the benefits of greater network stability would overrule this.

5.2.4. Enhancements for Evidence Storage and Report Generation

As has been mentioned earlier, the use of P2P overlays to assist in automating the generation of reports for digital investigations is limited. However, a case may be made for storing facts derived from the analysis phase within a distributed hash table (DHT) based overlay such as Chord. In this way the information is distributed to multiple nodes for redundancy purposes and is easily searchable. In this way report generation can be assisted through the search and retrieval of this data that is then compiled. The insertion of derived facts into a DHT for storage would be initiated by the peers performing the analysis. These stored data items would obtain an identifier from the process of hashing the actual data. The location where the hashed identifier would be stored would be determined through a suitably decided distance function such as that seen in the Chord overlay where the closeness in similarity of the hashes determines the storage location.

5.2.5. Enhancements for Remediation

The main focus of remediation is to facilitate some form of response or reaction to the malicious activity. As established earlier in this study, such actions are usually specific and directed and thus we propose the use of a publish-subscribe form of overlay where devices that are either evidence sources, or have been implicated in malicious activity are subscribed to response actions that are generated by the nodes performing the analysis of the evidence data. The enrollment to the response actions may happen during the triage, acquisition or the analysis phase depending on when an entity is determined to be implicated in the malicious activity. We propose the use of the SpiderCast[28] overlay due to its ability to route messages only through “interested” parties (thus fostering privacy), as well as its high resistance to churn. SpiderCast is also appropriate because of its “per-topic” overlay connectivity. This would be suitable as malicious activity usually has a motive and a target, which would correspond to a single “topic”; and it is uncommon to receive, multiple forms of attacks that are unrelated. Response action messages should also be encrypted and signed to avoid manipulation from unintended sources.

5.2.6. Support for Interchange of Structured Overlays and Self-Organization

Structured overlays are used so far especially in supporting triage and acquisition. Together with this, some of the DCXP protocol functionality can also be incorporated. As DCXP supports the interchanging of the underlying overlay as long as it is DHT-based, it can be seen that the Chord overlay could be substituted for another should there be a need based on further functionality needed. Furthermore context-sensitive self-organization of DHT-based overlays is also supported in the DCXP protocol, thus it can be seen that the overlay can re-organize the network so as to improve performance, or routing efficiency particularly for the acquisition phase.
As can be seen in Figure 2 the functionality of the centralized Cloud-based Back-end (CBB) and the Law Enforcement Controller can possibly be absorbed through distributing their capabilities among the HbH peers as well as with support from the super peers (HbH Master peers) that are equipped with more resources and better network stability.

6. Conclusions

Automating digital forensics and incident response mechanisms in loosely controlled networked environments is a difficult task to achieve. This is mainly because of the shared infrastructure, shared responsibilities, conflicting goals and the lack of trust in the other parties interacting within the loosely controlled networked environment, particularly with the service provider as they have privileged access to resources. Additionally, the availability of potential evidence sources is also seen to be a major problem as devices in such environments are in a state of flux in terms of their network connectivity. Furthermore devices common to such environments are often strapped for resources such as processing power, storage, working memory and battery power – which may also affect their availability. The strict requirements of digital investigations conflict with the characteristics of such an environment in that they require control, trust, stability and availability of potential evidence sources (suspected devices), as well as of the mechanisms used to facilitate the digital investigation. In particular, the evidence triage, collection, reporting and analysis methods used need to be highly trustable, reproducible and acceptable by the domain experts, as suggested by the Daubert Standard. The presence of large amounts of private data (either personally identifiable, or confidential company information) also poses a problem. This is because such data, otherwise considered private, may necessarily be implicated in criminal proceedings and thus a trade-off must be arrived at in which the data is held confidentially unless there is reasonable certainty that it is considered of evidentiary value.

In this paper we have identified the challenges facing tools for providing Digital Forensics and Incident Response (DFIR) services in loosely controlled networked environments such as deficiencies in availability, the lack of trust, the scarcity of
resources and the presence of lots of private data. Together with this we have also identified the challenges linked to the increasing amounts of devices and data generated in such dynamic environments. The need for scalability (upwards and downwards), the capacity to deal with heterogeneity, the need for automation of digital investigation mechanisms and collaboration among devices through commonly understood machine digestible formats have been identified. Consequently, from these challenges, we have identified the requirements for a system to be able to perform digital forensics and incident response in loosely controlled networked environments.

Further to this we have drawn from the field of peer to peer (P2P) networking in order to advance the field of digital investigations. The aims of most P2P overlays are underpinned with availability, scalability and performance in the face of unpredictable network churn, providing distributed services in a stable manner. That is, they provide stable services in an unstable distributed environment despite the lack of centralized control. Drawing from the strengths from different types of P2P overlays, we propose the use of multiple P2P overlays in order to support the different phases of the typical digital investigation process model. Through carefully selecting a combination of structured, unstructured and hybrid overlay topologies, based on their strengths in different areas, we proposed an architecture as well as enhancements to this architecture in order to provide capabilities that allow for enabling digital investigation in loosely controlled network environments. In this way we extend [21] and [22] by using multiple P2P overlays to provide decentralization and automation to more phases of the digital forensics process model.

7. Future Work

Though this use of P2P networks to support digital forensics and incident response is a step forward, there are still further improvements that can be made in order to truly achieve independent and automated digital investigations in loosely controlled network environments. For one, further study needs to be conducted into the cryptographic protocols to be used in order to achieve the necessary security that such a system needs. The use of a PGP public key infrastructure as well as threshold cryptography are being studied in order to integrate them into this architecture. In addition to this the actual implementation and testing of the actual overlays is yet to be done. This would enable us to practically determine the suitability of the chosen overlays for their respective designated functions. Finally, further benefits relative to P2P network self-organization may be derived through harnessing the information that they exchange.

Acknowledgments

Much gratitude to Theo Kanter, Rahim Rahmani, Panagiotis Papapetrou and the anonymous reviewers for the comprehensive and insightful feedback that helped improve this paper.

References


Authors

Irvin Homem is a PhD student at the Department of Computer and System Sciences, Stockholm University. He holds a MSc. degree in Information Security from the Royal Institute of Technology (KTH, Sweden) and has worked at Deloitte (Eastern Africa) as a Business Analyst. His current area of research focuses on the automation of digital forensics on mobile devices and cloud infrastructures using peer to peer networks, intrusion detection systems, hypervisors, big data processing frameworks and semantic web technologies.

Theo Kanter, earned a Ph.D. in computer communications, from the Royal Institute of Technology. Theo has held a number of leading positions in telecommunications research. From 1999 to 2007, he was a senior scientist at Ericsson Research. He is now a professor at the Department of Computer and System Sciences at Stockholm University, where he leads research in adaptive and context-aware mobile communication, service architectures and self-organizing application infrastructures.

Rahim Rahmani earned a Ph.D. in communications in heterogeneous networks and he is an Associate Professor of Computer Science at the Department of Computer and System Sciences at Stockholm University, where his research focuses on Collaborative ubiquitous services and context-aware mobile communication and service architectures and self-organizing application infrastructures. He is a member of the editorial board of International Journal of Wireless Networking and Communications.