INVESTIGATING IN THE CLOUD

As data moves from accessible data servers, mobile devices, and personal storage to cloud computing storage, fraud examiners will be required to locate evidence from the cloud. This session discusses, in a nontechnical manner, the new considerations that investigators might face, such as identifying the international legal jurisdiction where their data or evidence is located and the hazards that may be encountered while obtaining evidence. It also provides practical strategies that can be implemented to address the issues of locating and obtaining data and evidence from cloud platforms.

GRAEME EDWARDS, CFE
Detective
Queensland Police Service
Australia

Graeme Edwards is a detective in the Queensland Police Service Fraud and Cyber Crime Group in Brisbane, Australia. Edwards has been a member of the Queensland Police Service since 1999, having previously been a Detective in the New Zealand Police Service. He has been a specialist investigator of financial and cybercrime for approximately 12 years. He has conducted numerous investigations into financial and cybercrime and the effects on victims, as well as identifying new methodologies of criminal Internet use. Currently, he is in the final stages of completing a doctorate of information technology degree with a thesis on investigating cybercrime in a multi-jurisdictional environment.

INVESTIGATING IN THE CLOUD

NOTES

Introduction

The digital world that we reside in has changed dramatically over the past decade. It will also change more dramatically over the next decade as technology is used to develop even more complex and convenient devices to manage our lives. With the adoption of technology comes a certain level of risk in our personal and professional lives. We need to understand and balance the risks of new electronic devices against their conveniences. In essence, we must control technology rather than automatically adopt it and allow the technology to control us.

One of the most prominent technological advances in our daily lives has been in accessing, collecting, and storing electronic data. Technology that we used ten years ago is now a museum piece. In ten years, the technology we use today will also be in a museum. Where once our data storage methods required direct physical proximity, we now live in a world where people want to be connected to their data 24/7, regardless of where in the world they are, where their data is stored, or the form of device they use. With this convenience comes risk and, as fraud investigators, our knowledge of the risk environment needs to work alongside our knowledge of these new technologies.

The information technology industry has met the desire for instant connectivity with the creation of vast data storage networks called *cloud computing* where users can obtain access to their data using multiple access devices from any connected network. The days of corporate data stored in the same building as the users of that data are fast disappearing.

Cloud servers are unique to any other form of storage traditionally used, and the manner in which the cloud

provider stores, moves, and recovers data requires those involved in using electronic evidence in their investigations to reconsider the manner in which they locate, seize, and present evidence in court. As fraud investigators, our job is evolving at the pace of new technology. The criminal community adapts technology as soon as it is released, and we must ensure that as investigators we are as adaptable and knowledgeable as the criminals.

There are many configurations in the way cloud service providers store clients' data, and this paper provides a very generic view. This is about where cloud data is stored in a public cloud configuration, where client data is stored and processed on shared services (multi-tenancy), and how the data is stored in a dynamic manner across multiple servers potentially across many different legal jurisdictions (multi-jurisdiction). It is acknowledged that law enforcement and civilian investigators have different legal instruments and levels of resources available to them to investigate financial crime. This paper attempts to provide a generic view of conducting an investigation in a cloud environment.

What Is The Cloud?

The official definition of cloud computing provided by the United States Department of Commerce National Institute of Standards and Technology (NIST) identifies the following features that a cloud computing service provides:

- Always accessible
- Convenient to access
- On-demand
- Shared resources (multi-tenancy)
- Elasticity (use only what you need when you need it)

(Mell & Grance 2011).

NOTES

Cloud services come in different shapes and sizes depending on the requirements of the client. Whilst one client might want data stored only in his legal jurisdiction, another client will not have this concern, and his data will end up spread out and moved throughout the world. Pricing is often a major consideration for corporate entities deciding to move their data to the cloud, and the cheapest option is not always the friendliest for an investigator.

Cloud computing uses massive data centres located throughout the world to store clients' data. Microsoft's cloud incorporates more than 100 data centres with more than one million servers in many different locations (Microsoft 2015). The data in a cloud environment might be constantly on the move and might not stay in one location for more than a microsecond before the network moves it to a more convenient location. The data the client places in the cloud might be spread across the many data centres in different countries depending on the storage rules of the cloud provider and, unless specifically included as a condition in the End User License Agreement (EULA), may not be in one single legal jurisdiction (Reilly, Wren & Berry 2011).

The boundaries of cloud storage are being reexamined each day, and the manner in which our data (potential evidence) is being stored places new challenges on investigators to understand and work within this technology.

How Did We Get Here?

Within recent memory, the 5 ¼-inch floppy disk was state of the art electronic storage. It was a giant step up from magnetic tapes, and the element of storage mobility was introduced to a commercial market. As technology progressed, the 3 ½-inch storage disk replaced the 5 ¼-inch floppy; many computer users might remember using a

NOTES

handful of these disks to load their operating systems onto DOS computers.

As technology developed, so did clients' storage requirements; having a handful of disks to load applications and save data became less convenient as users' requirements for off-server storage increased. CDs came next with their rewritable ability, and then we saw the arrival of the DVD with its increased data storage capacity. Law enforcement investigators will recall seizing many hundreds of CDs or DVDs from a suspect's address and then having to examine each one individually for evidence.

All this time, investigators and forensic examiners have had to adapt with the changes in technology. The capacity of data storage changed again with the introduction of USB devices and portable drives. At one time a backup up portable drive could hold 200MB, but the reduction in the price of storage and the increase in technology resulted in portable drives that could carry 2TB in a person's pocket or bag. For investigators, the size of the task we have in locating and processing digital evidence is getting larger and more complex as the potential to individually review each file, document it, and create a spreadsheet on a seized drive might go beyond the capacity to allocate resources, except in the most serious of cases.

What Is This Relevance to CFE?

As technology develops, the investigator must progress along with it. Investigators do not have any choice but to keep up with technology, because the criminal community researches new technology as soon as it is released with an eye to identifying how it can be used to commit crimes. Data storage is important for the white-collar criminal as the getaway car is important to the bank robber.

NOTES

NOTES

We must appreciate that the methodologies we use to investigate financial and cybercrime are constantly evolving, and the way we conducted our investigations yesterday might not be relevant today or tomorrow. The cloud stores not just the client's data, but also our evidence. It can be spread across many different legal jurisdictions that cannot be initially identified without the support of the cloud provider. The evidence of that financial crime being investigated might be spread across 20 different computer servers in 15 different legal jurisdictions.

As financial crime investigators, we need to ensure that the evidence in the cloud is accessible, and this will take considerable pre-planning and an understanding of where the technical and legal environment of the cloud industry has taken us. At one time, auditors and investigators looking into a failed company only had to ensure that the rent and electricity were paid so that the investigation could be undertaken, but now the investigator must also ensure that the cloud provider is paid or else the evidence might be lost forever.

Today, there are pitfalls we must factor into our existing investigation plans. If there are different legal jurisdictions involved in obtaining evidence, then we must respect those laws and ensure that our evidence collection methodologies adhere to the laws legally and ethically (Ruan et al 2011).

Where Do We Currently Obtain Electronic Evidence?

Electronic storage is everywhere we look. It is now wearable in the form of watches on our phones. Our electronic evidence can now be located anywhere in the world, and the days of financial crimes being committed solely in our jurisdiction are coming to an end. Where we

could once serve a search warrant on an address or a court order on an individual to locate our evidence now, with cloud computing, our evidence may be located in foreign legal jurisdictions or split amongst many. The many different data storage devices we have been using are being retired by the industry and, soon, when we examine a suspect's computer, mobile device, or otherwise, there is the potential for limited to no evidence immediately accessible except through log records pointing to the evidence located in the cloud.

Currently, most of our evidence is located within physical proximity. We can collect it and hand off the digital evidence to examiners who then prepare the evidence for examination. Even within our own organisations, evidence is being stored on cloud servers, so an internal investigation might encounter cloud computing related barriers.

Remote storage also creates a situation in which the investigator seizes an electronic device and the owner remotely removes the evidence whilst it is in the investigator's possession. Examples include mobile phones, tablets, and cloud evidence.

Understanding the changing face of financial crimes

Professional Nature of Financial Crimes

Financial and cybercrime is becoming more professional. Those tasked with investigating large complex financial crimes committed by unknown external parties are likely to find they are facing anything from an individual, a loose network of associates, or a highly sophisticated corporate style structure incorporating R & D departments and specialists in many different areas involving financial crime.

NOTES

Financial criminals within an organisation may seek specialist advice external to the organisation to learn new methodologies to commit their crimes and eliminate the evidence. Criminal dark markets exist, and tutorials are provided on how to commit financial and cybercrimes. With the rapid rise of new technology and professional criminals offering to provide their services on a contract basis, the internal criminal now has the opportunity to defraud his employer or clients using a level of sophistication not previously had. Alternatively, the internal criminal can contract a third party to commit the crime for him, such as with the theft of corporate intellectual property.

The criminal community has created markets to purchase and sell criminal products. Data stolen from corporate networks are keenly sought and are currently a niche market. Personally Identifiable Information (PII) is traded on a daily basis, and the proceeds of the financial crime the CFE is investigating might end up traded on the dark markets. To provide an understanding of where the proceeds of corporate crime can end up, we will quickly view the dark markets and show a practical relevance of this cyber technology and its relevance to CFE and other financial investigators.

Dark Markets

These markets are created by the criminal community for the criminal community. They are structured like online auction sites where vendors advertise their criminal products as services, such as hacking for hire and stolen corporate or personal data. Traders rate each other and provide feedback on the credibility of the other criminals and the quality of their products.

NOTES

Other services the sites provide include support services, arbitration in the instances of a dispute between a vendor and purchaser, and open forums where criminals discuss the latest technology and methodologies to commit financial crimes. In some instances, markets may provide a support service to those who are having difficulty committing their financial crimes.

These markets also provide training material available to those seeking to commit a financial crime. Step- by-step instructions are provided on how to commit crimes against employers through external attacks on companies to obtain financial information to on-sell to competitors.

The relevance of this to the CFE is that the criminal community is stepping up its skills in committing financial crimes against industries and individuals. They are using new and emerging technologies, such as cloud computing, to commit or facilitate these crimes from many different legal jurisdictions, thus making the CFE's job harder. Dark markets and cloud computing technology can merge to make the investigator's job far more complex.

The following section presents a case study of employee Intellectual Property (IP) in which the stolen IP was hidden in a multi-jurisdictional cloud-computing environment. Using this case as a reference point, we will discuss the unique features that cloud computing presents to investigators, and then we'll present a series of considerations that may assist investigations.

NOTES

Case Study

In 2013, the Queensland Police Service Fraud and Cyber Crime Group received a phone call from a distressed owner of a company where a former employee had allegedly taken $15 million of IP after resigning from his job after an argument with the company owner. He had taken the IP and sent it to his cloud storage device in the minutes prior to leaving the office for the final time. The public release of this data or the selling of it to a competitor would have meant the loss of 15 years of work and approximately 100 jobs.

The cloud storage provider was based in a foreign country, and it was not known in which or how many countries the data spread to. It was also unknown how many copies of the IP he had, as from the time of stealing the IP until police executed a search warrant at his address, he had several hours to access, copy, and forward the IP to other storage.

The following section will introduce some of the unique features regarding cloud evidence that an investigator may have to consider. In each instance, the feature will be related back to the case study to provide a practical example.

Unique features of cloud computing for an investigator

1: Where Is the Evidence and How Can I Get It?

Identifying the jurisdiction is a major consideration when locating cloud evidence. Your evidence might be located in your jurisdiction; however, it might be located on many different servers in different data warehouses across many different legal jurisdictions (Ruan et al 2011). There is no guarantee that all of your evidence is in the one location. Cloud computing does not work that way. One cloud provider interviewed said

NOTES

a client's data might be spread across 23 different data centres in 15 different legal jurisdictions, or the data might be located in only one data centre. They cannot tell until they look themselves.

To find out where your evidence is, ask your clients in the first instance what form of agreement they have with their cloud suppliers. Some agreements stipulate the evidence will not leave their jurisdictions; however, others allow the data to be in any location the CSP dictates. Some might have an agreement on how incident management response and support are provided.

If you are unable to find it, you may ask the CSP legal department for assistance. CSPs have stated that if a customer or agent requires evidence from their client servers, they would like to be contacted in the first instance to preserve the evidence. They can advise what evidence is available and the method in which it can be obtained.

CSPs have complained in the past that the court orders they have been served often make no sense, directs them to supply data that another law specifically forbids them to supply, or requests only a fraction of the evidence that is available.

In some instances, if the evidence is spread across multiple legal jurisdictions, multiple legal applications are required to obtain the data.

Case Study: The evidence was fortunately located in only one jurisdiction—the United States.

NOTES

NOTES

2: Volume of Data Storage

The volume of data stored in the cloud is increasing exponentially. It is approaching the stage where it is very difficult for an investigator to conduct a full examination (Thethi & Keane 2014).

Investigators need to know that when they seek and obtain cloud-based evidence they may require significant resources to support the receipt of large volumes of data and the associated applications required to review it.

This is becoming such as issue that some cloud providers have said that despite any court order served on them, they will not provide evidence beyond 1TB because of the cost and time involved in conducting the forensic image.

Plan specifically for the evidence you need, and communicate with the CSP about what can be done to ensure that the data you seek is justifiable in court and can be managed upon receipt.

Case Study: The evidence was less than 1GB, so storage was not a consideration in this instance. Other IP located on the suspect's home computer identified several hundred megabytes of other IP taken from the company using portable storage.

3: Chain of Custody

If there is an intention to produce evidence in a court hearing, a requirement is to account for the evidence from the time of creation to production in court. This is called the *chain of custody*. With cloud computing, this might involve significant planning and the requirement to obtain court statements from multiple persons in the

CSP as well as other parties involved in the data collection process such as legal representatives.

> *The chain of custody is a document identifying the chronology of the movement and handling of the potential digital evidence. It should be instituted from the collection or acquisition process (ISO 2012 p.10).*

When evidence is obtained from cloud servers in different countries, several persons from the organisation may need to provide support to ensure that the evidence is successfully presented in court. Some law enforcement agencies fly their examiners to the cloud provider so that the examiners are present when the evidence is obtained to preserve the chain of custody.

Case Study: The cloud provider was very supportive and prepared to provide statements as required.

4: Mutual Assistance in Criminal Matters Treaty

For law enforcement officers, a Mutual Assistance in Criminal Matters Treaty application is required to seek cloud-based evidence. This is a time consuming and cumbersome process that may require multiple MLAT applications to obtain evidence. Once the evidence has been received, further inquiries involving further MLAT applications might be needed.

MLAT applications can take up to 18 months to obtain the evidence.

Case Study: An MLAT application was required to obtain the evidence in this instance.

NOTES

NOTES

5: Cloud Forensics

In traditional investigations, investigators have direct access to electronic evidence. A forensic examination is undertaken on digital evidence, and this evidence is used to progress the evidence.

There have been considerations amongst forensic examiners and academics about the potential to conduct a forensic computer examination on a cloud server in a foreign legal jurisdiction (CSA 2013). This is to locate and obtain evidence in a prompt manner and to advance the investigation.

This methodology is considered very dangerous to the examiner and the investigation team and, as with cloud computing, there is no clear way to know where the evidence is at the time of the investigation. Should the evidence be removed from a country with specific legislation barring such an external investigation and prohibiting the removal of data from that country, then the investigation team may be subject to a criminal investigation and prosecution in that jurisdiction. Examples of these countries include Germany, France, and Russia. In fact, the European Union as a whole is very protective of data stored in its jurisdictions, and serious penalties exist for those who breach European laws.

One CSP attempted to conduct a remote forensic computer examination on its own computer containing its own data placed there by employees in Europe. The CSP was then informed by that jurisdiction's law enforcement officials that it was committing a criminal offence. Subsequently, the CSP stated that if there's a problem with computers in foreign jurisdictions, it

would rather fly a forensic examiner to that place rather than consider a remote forensic examination.

A remote forensic examination also only obtains a portion of the evidence. As the client does not have any access to the infrastructure of the cloud provider, log evidence is available that might be valuable to the investigation that cannot be accessed without the explicit support of the cloud provider (Krotoski & Passwaters 2011).

Furthermore, conducting a remote forensic examination on a multi-tenancy environment has the potential to damage the provider's and possibly clients' data. This may render the investigating authority open to civil liability.

CSPs are also adamant that they will not allow any person or authority to conduct a remote forensic computer examination on their servers. There are to be no exceptions to this rule as they believe they do not know who is doing the examination, what their qualifications are, whether it is a justified examination, or whether it's a computer hack. Further, they do not want an examiner reaching into their proprietary infrastructure seeking network logs and potentially causing damage to the infrastructure or client data.

Case Study: Remote forensic examination was not considered because of concerns about the location of the evidence at the time of the examination, lack of access to network side logs, and the inability to present the evidence in court to the standard required. There was also a concern about not having the cloud provider's agreement to conduct such an examination.

NOTES

NOTES

The legality of the action may have been challenged in court.

6: Resellers

Cloud providers sell their services to other cloud providers. For example, Dropbox is a large cloud provider; however, it hires cloud services from Amazon Web Services and does not own its infrastructure (Dropbox 2014). There are many cloud providers that provide cloud services, and there are several layers from the company providing the cloud infrastructure and associated architecture. This raises the issue for the CFE as to where to get the evidence: From the reseller providing the content evidence or from the original company providing the infrastructure with the log evidence? Maybe both?

Although this will be addressed on a case-by-case basis, speaking to the CSP will provide information on who can provide what information. As a starting point, consider obtaining content evidence (documents, etc.) from the reseller, and speak to the infrastructure provider to see what logs or metadata it can provide.

One problem with resellers is that the smaller they are, the less likely they are to record the evidence you need. Recording and subsequently storing logs can be very expensive for a smaller cloud provider. They may also lack the capacity to secure electronic evidence when requested in a forensically sound manner.

Some cloud providers include in their terms and conditions a requirement that once a client places data in the supplier's cloud, ownership of the data changes to the cloud provider. This is not always the case, but there are providers that include this condition in the

End User License Agreement as they are aware that clients never read the conditions and "tick and click" the agreement to commence the service. This is more common amongst resellers than amongst the major cloud providers. This may affect your evidence as it may reduce the possibility for your client or complainant to give consent to access what they believe is their data.

Case Study: The cloud provider was not a reseller. If it were, then MLAT agreements would have been sought for the content data from the reseller and the log data from the infrastructure provider.

7: Deleted Evidence

Deleted evidence incorporates several possibilities.

1. Memory stored in short- term memory (Random Access Memory) is overwritten very quickly after being deleted. For CSPs operating on multi-tenancy where millions of clients are potentially sharing the same infrastructure, if a client or suspect deletes data stored in random memory (RAM), the reality is that it will be overwritten before it can be accessed, and it will be lost.
2. CSPs operate on virtualisation, and the data is represented in virtual form. Examples of virtualisation include popular products such as VMware. Should an offender or client shut down the VM server/ instance, crucial evidence is destroyed. Do not consider shutting down a machine in which digital evidence may be resident without obtaining specialist advice and support.

Case Study: The evidence was promptly located in the suspect's cloud account, and he had not copied it or

NOTES

moved it to another location. If it had been deleted, this form of evidence would not have been recovered.

8: Computer Logs

Computer logs can be crucial evidence in a financial crimes investigation, and an understanding of what logs are available and what they mean can be the difference between proceeding with an investigation and not proceeding. Log evidence in some instances can be as conclusive as fingerprint evidence in court. CSP might be recording this evidence, so understanding what you can access and following the evidentiary trail can be very beneficial.

Case Study: The log evidence at the complainant's address and on the suspect's computer pointed directly to the cloud provider where the suspect had a storage account.

9: Production of Evidence In Court

Legal systems throughout the world operate on different principles of law. Case law is established underneath legislation, and courts develop the rules on how evidence is to be collected, preserved, and presented. As financial crimes investigators, we must ensure every action we undertake in an investigation passes the legal and ethical standards required by the courts.

Because cloud evidence might be distributed throughout the world and difficult to obtain in a timely manner, it is important to consider right from the commencement of your investigation adherence to the rules of evidence in your jurisdiction. The evidence that you seek is difficult enough to locate and obtain

NOTES

NOTES

without it failing to be accepted as evidence in a prosecution.

There is no substitution in your pre-investigation plan for the failure to plan for placing emphasis on the quality of your evidence and its admissibility in court if it is challenged

Case Study: Support was provided by the cloud provider.

10: Cost Of an Investigation

When a CFE is required to conduct an investigation seeking cloud-based evidence in a foreign legal jurisdiction, there may be a significant financial cost involved in obtaining court orders to get the evidence. In the U.S., a formal court order is required, and a civilian investigator can only obtain non-content data from a suspect account. MLAT applications are only available to law enforcement investigators.

Budgeting for the cost of an investigation is a consideration of the pre-event investigation plan in which the cost of an investigation can significantly exceed that of the offence being investigated.

Case Study: The case resolved with admissions of guilt early in the investigation process.

Investigation Tips

As each investigation is different and legal jurisdictions adhere to different laws, the tips provided here are generic and provided as a guide for your information. Not all of these tips will be relevant to your investigation or jurisdiction; however, they might provide some assistance or direction.

NOTES

1. Develop an investigation plan prior to undertaking any investigation involving cloud-based evidence. Your cloud evidence may have a short life span, and you may not have the time to consider the many unique factors that cloud evidence involves. Your investigation plan will start prior to an incident (identifying specialist support) occurring and following through to the production of evidence in court.
2. Know your CSP. If you are in an entity that has your data in the cloud, know who your CSP contacts are in the event of an incident and how to contact them in an emergency. Discuss the process of evidence recovery before the event, including what evidence they can provide and how it can be obtained.
3. Know your jurisdictions. If you are an entity with data in the cloud, know where your evidence is likely to be stored. Major CSPs offer services so that your data will never leave your jurisdiction, making subsequent investigations less complex.
4. If you are in a position in which you are likely to be seeking evidence on behalf of a client, consider whether you have the storage and associated resources available to manage the large volumes of evidence that cloud computing can produce.
5. Investigations involving cloud-computing evidence can be very expensive depending on where the evidence is located and your ability to access it. Civilian investigators may be required to contract legal support in foreign jurisdictions to obtain evidence when the evidence is in a cloud service not belonging to the client or when a court order is required to recover your own data.
6. Act quickly to preserve data and evidence.
7. Know where you want to end up. Is your investigation for a criminal or civil court? Is your investigation of an

incident for a tribunal hearing or to identify what went wrong and the extent of the damage? Knowing this will allow you to allocate resources and implement your strategy more effectively. If unsure, plan your investigation for the most serious court hearing where your evidence and its collection will face the most scrutiny.

8. Remote forensic examinations: This is a potential danger to your investigation and the personal integrity of the examiner. Do not even consider this option without the consent of the CSP, the data owner, and without understanding the legality of the action in the jurisdictions where evidence is located. There is a lot of homework required before even considering this option.
9. Should this evidence be presented before the court, consider the assistance of an independent expert who can explain the technology to the court before the introduction of evidence. An independent expert can bring credibility and an added level of transparency to the cloud evidence.
10. Validate the evidence. To add strength to the cloud evidence, corroborate the evidence against evidence from traditional sources. Examples include logs from electronic devices found on the suspect or defendant, copies saved by the suspect or defendant, or admissions made.

Summary

Although cloud based evidence provides financial and cyber investigators new challenges that need understanding, there is no reason why evidence cannot be located, seized, and presented before the court in a manner that abides by the rules of evidence. The courts are continually dealing with complex new technologies and, as time passes and we get more comfortable with the technology, lessons will be learnt and dealt with.

NOTES

NOTES

The most important tip is to have an investigation plan prepared and tested before the event occurs.

References

Cloud Security Alliance, 2013, *Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing* [Online], Available: cloudsecurityalliance.org/download/mapping-the-forensic-standard-isoiec-27037-to-cloud-computing/, [Accessed 28 February 2015].

Dropbox at AWS re:Invent 2014 (2014), [Online], Available: blogs.dropbox.com/tech/2014/12/aws-reinvent-2014/, [Accessed 10 September 2015].

Krotoski, M.K. & Passwaters, J. 2011 'Obtaining and admitting electronic evidence', *The United States Attorney Bulletin*, vol. 59, no.6, pp. 1-15.

Mell, P. & Grance, T. 2011, *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology* [Online], Available: csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, [Accessed 10 September 2015].

Reilly, D., Wren, C & Berry, T. 2011, 'Cloud Computing: Pros and cons for computer forensic examination', *International Journal Multimedia and Image Processing (IJMIP)* vol. 1, Issue 1, pp. 26- 34.

Ruan, K., Carthy, J., Kechadi, T & Crosboe, M. 2011, *Cloud forensics: An overview* [Online], Available: www.cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf, [Accessed 10 January 2012].

We power the Microsoft cloud (2015) [Online], Available: www.microsoft.com/en-au/server-cloud/cloud-os/global-datacenters.aspx, [Accessed 10 September 2015].

NOTES