T847 MSc Professional Project

Investigation on Challenges Introduced by Cloud Computing on Digital Forensic Processes and its Impact on the Effectiveness of Current ACPO Principles

Kareem El-Farargy

F66 MSc Computing (Information Security & Forensics)

End of Module Assessment (EMA)

07 April 2022

CONTENTS

EXECUTIVE SUMMARY

Cloud computing and its growth in popularity, technological advancement and expertise has resulted in the transformation of the use of physical infrastructure to virtual and remote cloud environments. These developments have generated a debate on traditional digital forensic processes, including the Association of Chief Police Officers (ACPO) guidelines, and if they remain relevant and proper. The research therefore presents an opportunity answer the following research questions:

RQ1 – What are the current challenges of Digital Forensics within the Cloud?

RQ2 – Are the current Association Chief Police Officers (APCO) guidelines sufficient in ensuring the collection of evidence within the cloud?

RQ3 – How effective would the principles proposed by Horsman (2020) be in addressing the challenges of cloud forensics?

The literature review sets the scene and gives a sense of the ongoing debate within the academic community. The review highlights 3 categories of challenges that cloud computing introduces to digital forensics. These are technical, legal and resource issues in attaining and preserving evidence within cloud environments.

The research involves primary data from practitioners and professionals within the IT industry contributing to key aspects of the debate and triangulating these to provide initial conclusions and recommendations. The structure of the primary research is a questionnaire responded to by 25 participants and follow up interviews with 4 participants.

Questions formed in the questionnaire on challenges within cloud computing were based on the literature review and whether current ACPO principles are fit for purpose. Furthermore, participants were asked to respond to the usefulness of a proposed framework in response to these challenges.

Data from surveys were used to probe opinion further with 4 interviewees, on arguments presented by Horsman (2020). The significance of the paper from Horsman (2020) is that it argues ACPO principles require updating and proposes 8 new principles to replace ACPO in response to the challenges cloud computing brings.

Both descriptive statistical and thematic analysis were applied to draw conclusions and recommendations from questionnaire and interview data. Respondents of the survey ranked multi-jurisdictional issues offering the biggest challenge, followed by ensuring data avoiding contamination and maintaining integrity in the chain of custody. While respondents were differing in opinion whether ACPO principles are outdated, the vast majority agreed that the sample proposal provided from Horsman (2020) would be beneficial to be included in future frameworks.

Given the majority agreeing with a sample of Horsman (2020) principle, the full 8 principles were probed further with interview participants. 4 of the 8 principles were in agreement of benefitting digital forensic processes in response to cloud computing challenges but the caveat is the potential complexity and complication they bring applying these in reality.

It is the complexity and global reach of issues within cloud computing that invokes debate without much agreement over the last decade. As it stands, there is still no formal update to ACPO principles due to the complicated nature of these challenges. The recommendations found by this research were as follows:

- Organisations that use cloud computing should ensure understanding of in scope jurisdictions and have associated legal representation in these areas.

- The ACPO guidelines are at risk of being outdated and not keeping pace with cloud computing developments. A further review of ACPO is recommended to adapt to this.

- Proposals from Horsman (2020) to update ACPO have value and credence however care is needed to avoid complexity with further research needed to balance this along with the need to respond to newly created challenges.

On reflection, there is little doubt Cloud Computing has changed how IT solutions are implemented moving away from traditional physical hardware to cloud service providers. The outputs from this research debates the impact of these changes on digital forensic processes many of which were designed prior to cloud computing.

However, the complexity of these challenges should not necessarily complicate further digital forensic guidelines but the existing challenges risk the relevance of ACPO principles being outdated or unable to keep pace. A balancing act is most likely needed to update ACPO guidelines in response to challenges and keeping the simple nature of them intact. Horsman (2020) makes a start on this and acknowledges it is open for criticism but it is these types of discussion that are required for any update to guidelines being in place in response to challenges around forensics within the cloud.

1. Introduction

The growth of cloud computing combined with cloud forensic practices, or lack thereof, are increasingly being debated given the challenges cloud computing brings to traditional digital forensic processes (Purnaye and Kulkarni, 2021).

The increase in popularity of virtual cloud computing over the last decade (Purnaye and Kulkarni, 2021) introduces these challenges for digital forensic practices that traditionally rely on securing physical devices having a chain of custody. Typical guidelines for current practices are defined under the Association of Chief Police Officers (ACPO) which aims to preserve evidence without compromise and maintain its integrity (Almulla, Iraqi and Jones, 2014).

Researches have agreed with the timely need for experts and processes to be in place for successful cloud forensics in today's ever increasing digital world and aid the ability to counter computer crime (Jain and Mahalkari, 2019) (Fernandes *et al.*, 2020). Previous market research has shown cloud computing is expected to grow at a 30% compound annual growth rate (Rani and Sravani, 2016) and claims this growth is exceeding that of digital forensic processes within the cloud presenting potential accountability gaps.

The widely practiced ACPO principles for digital evidence have been challenged in its validity and relevance given it has remained fairly unchanged in the last decade (Horsman, 2020). With no clear successor to a standard framework mitigating the shortcomings of the 4 ACPO principles (Horsman, 2020), the research aims to contribute to the theory and practice identifying solutions and its effectiveness in forensically accounting for activity within the cloud.

The focus and motivation of the research are therefore around cloud computing in relation to digital forensics, its challenges and whether current practices such as ACPO are fit for purpose. Montasari and Hill (2019) comments on example challenges using terms such as multi-tenancy and multi-jurisdictional issues that require a new dimensional approach (future paradigms) to digital forensics. Chen et al, (2019) echoes the difficulty in detecting malicious activity in the cloud.

Summarising the introduction and importance of the growth in cloud computing and its impact on associated forensic capability, there is potential scope to contribute improvements of theory and practice against the arguably aging digital forensics methodology currently in place. Organisations that migrate its systems to the cloud should also consider its accountability of its forensic capability ensuring its awareness.

1.1 Background

Initial observations from literature searches around digital forensics within the cloud and developments in the area had a number of references to a particular bold quote from Gartner: Seven cloud-computing security risks (Sang, 2013), (Pătraşcu and Patriciu, 2013), (Guo, Jin and Shang, 2012):

"*Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible.*" (Brodkin, J., 2008. Gartner: Seven cloud-computing security risks. Infoworld, 2008, pp.1-3.)

Additionally, literature challenging the validity of current digital forensics frameworks (ACPO principles) in light of cloud computing developments (Horsman, 2020) provide further stimulus in identifying a significant problem. Researches have cited Horsman's (2020) concerns that ACPO methodologies are outdated and the requirement for the digital forensic industry to adapt (Findlay, 2021). Recognising this problematic trend led to a wide range of academic literature commenting on the challenges, potential solutions and proposed frameworks of digital forensics within cloud computing.

As an initial basic definition, the science behind digital forensics is the identification, collection, organization and presentation of evidence (Zawoad and Hasan, 2016). This definition can be expanded to include the validation, analysis, interpretation and documentation of digital evidence (Marturana, Me and Tacconi, 2012). The ultimate aim behind digital forensics is to answer the 5W's - Why, When, Where, What and Who (Miranda Lopez, Moon and Park, 2016).

The growth in the adoption of cloud computing by organisations is driven by scalability, convenience, cost efficiency with the market being in the billions and growing (Vu, Hartley and Kankanhalli, 2020). The radical change in paradigm in cloud computing, where software and data move from traditional physical locally hosted devices to cloud service providers on the internet introduces complications to traditional digital forensic methodology (Montasari and Hill, 2019).

1.2 Challenges

For digital evidence to be forensically sound, meeting technical requirements isn't the only goal, but to legally uphold admissibility in courts of law (Morioka and Sharbaf, 2016). The risk of international collaboration, complexities and multitude of data evidence adds complication of meeting legal jurisdiction requirements in a timely manner (Irons and Lallie, 2014). Furthermore, cloud computing is multi-tenanted in nature where hosts can have multiple-tenants sharing storage/memory and networks making forensics complicated (Pichan, Lazarescu and Soh, 2015).

Digital forensics requires to keep up with evolving cloud computing advances (Sibiya, Venter and Fogwill, 2012). Sibiya, Venter and Fogwill, (2012) summarises these challenges below:

CHALLENGE	DESCRIPTION
Identity	It is hard to link data stored in the cloud to an individual cloud user
Encryption	Data encrypted by the client before sending it for storage and further by the cloud service provide before storing it
Jurisdiction	Accessing data stored in computers beyond local borders may violate laws in other countries
Distribution	A cloud user may distribute data in several countries hence collaborating with each of these countries may be costly.

Table 1: Sibiya, Venter and Fogwill, (2012) - Digital Forensic Framework for a Cloud Environment – p4

Guo, Jin and Shang, (2012) summarises similar challenges in cloud delivery models. While the summary of cloud model forensic challenges from Guo, Jin and Shang (2012) appears reasonable, its conclusion is derived from a newsletter source leaving it open to challenge. The lack of evidence as to why each of the points mentioned is a challenge and their hindrance to forensically sound evidence provides a weak argument as a result of its omission in depth of research.

In contrast, the approach taken by Al Fahdi, Clarke and Furnell, (2013) identifies challenges within digital forensics in general through a survey of researchers and practitioners. Al Fahdi, Clarke and Furnell, (2013) also agrees that challenges are both technical and legal of nature however adds another dimension of challenge – resources, e.g., time to analyse in relation to acquiring volumes of data.

A total of 19 academic researchers and 23 practitioners responded to the survey which aimed to gather challenges within the digital forensic space overall. Some of the key findings are illustrated below:

Figure 1– Technologies of concern - Al Fahdi, Clarke and Furnell, (2013) Challenges to Digital Forensics – p3

IMAGE REDACTED FOR COPYRIGHT REASONS

Out of the areas of concern, Anti Forensics, Cloud Computing, Pace of Technology Change, Malicious Software, Encryption, Steganography and Privacy Enhancing Technologies - a significant percentage of respondents identified the concern around Cloud Computing as well as Pace of Technology Change.

However, what gives further credence to the challenge of forensics within Cloud Computing is the ranking of future challenges out of all the above areas of concern:

Figure 2 – Relative Ranking of Future Challenges - Al Fahdi, Clarke and Furnell, (2013) Challenges to Digital Forensics – p5

The findings from Al Fahdi, Clarke and Furnell (2013) corroborate with the conclusions from Guo, Jin and Shang (2012) and Sibiya, Venter and Fogwill, (2012) albeit through different means. Furthermore, the pace of change in developments in itself is seen as a particular challenge echoed by findings from Purnaye and Kulkarni, (2021) with the increase in cloud adoption and increased expertise naturally adding to existing challenges.

IMAGE REDACTED FOR COPYRIGHT REASONS

The challenges remain to be highlighted by Fernandes *et al.*, (2020) who categorises these into the Identification, data collection and preservation stages of the forensic process:

Stage	Challenges
Identification	Retrieval of evidence from cloud logs Data volatility Service Level Agreements
Data Collection & Preservation	Data Integrity and Stability Time Synchronization Privacy Chain of Custody Multi-Jurisdictional Issues multi-Tenancy

Table 2: Fernandes et al (2020) Summary of Cloud forensic challenges

In-line with categorisations from Table 1, many of the challenges identified by Fernandes *et al.*, (2020) – such as jurisdictional, identification and chain of custody issues appear to persist and remain over the last decade.

1.3 Potential solutions

Whilst most commentators agree on the challenges of the problem, the approach to solutions to mitigate are more varied in opinion. Sang, (2013) argues a log-based approach towards accountability and nonrepudiation. However, the key argument is not relying on 3rd party vendor for logs but by synchronising associated logs stored locally. Sang (2013) accepts the limitations of this concept, mainly depth of forensically required audits, but argues this is a step towards the lack of guidelines within cloud security.

Rani and Sravani, (2016) acknowledges both the log-based approach and the lack of standardised frameworks for cloud computing. They propose an additional solution where a dedicated Virtual Machine (VM) is selected to "police" suspected VM's and take a snapshot capturing all relevant evidence to store in persistent non-volatile storage. Similarly, the paper acknowledges the limitations of this solution where snapshots are not a true replication of the scene and therefore might face legal scrutiny.

In contrast to logging and snapshot solutions, research into an automated detection design to monitor activity over the cloud as well as detecting malicious activity (Pătraşcu, Velciu and Patriciu, 2015) providing reliable and secure evidence. The experimental approach taken by Pătraşcu, Velciu and Patriciu, (2015) aims to demonstrate pro-activeness and automation to mitigate the challenges posed by cloud computing. The limitations of the experiment are restricted to proof of concept and more complex reflective real-life situations is needed to add authority to its solution.

Fernandes *et al.*, (2020) highlights multi-jurisdictional issues remain challenging, however encourages greater collaboration between cloud providers and consumers engaging in an improved partnership concluding that the challenges are still a work in progress.

1.4 Proposed frameworks

The discussed solutions in isolation may not be enough to combat the challenges of cloud forensics, updates to frameworks and guidelines such as ACPO are recommended to pursue standardisation of practices (Zargari and Benford, 2012) to encourage adoption. Zargari and Benford (2012) argue that traditional digital forensic practices are inadequate to apply to cloud forensics. Horsman, (2020) echoes this sentiment and radically proposes 8 new principles to meet cloud forensic challenges – these are provided under Appendix I.

In contrast to Horsman (2020), Martini and Choo (2012) stipulates that a re-invention of the wheel is not required but an integrative and iterative approach to the current frameworks of McKemmish (1999) and NIST (Kent et al., 2006) can be utilised to mitigate the problem. Martini and Choo, (2012) proposal is conceptual and aims to validate its recommendations by further survey research. Horsman (2020) proposal is motivated by the fact that there has been no significant change in ACPO principles in the last decade despite the pace of new technological developments. It aims to highlight that the current framework is not fit for purpose and be open for debate rather than promote its own principles.

1.5 Introduction Summary

It can be surmised that digital forensics within cloud computing introduces complexities and a source of debate within researchers. Despite a number of varying solutions and proposed frameworks over the last 10 years of research, as commented by Purnaye and Kulkarni, (2021), it remains a niche area with scope for agreed standards to be established in future.

Additionally, the lack of progress on addressing these challenges can be derived from commentary on the same challenges over the equivalent time period. The implications of potential forensic gaps and lack of standardisation highlights the importance of the need to review challenges and ensure integrity of the digital forensic processes. Relevant organisations and law enforcement also should increase awareness utilising and analysing cloud solutions.

2. Project Evaluation

2.1 Personal and Academic Suitability

The suitability of this research is aligned with ongoing debates that are happening in academic literature around challenges within cloud computing and associated forensics.

With a personal academic background and interest in Systems and Information Security in addition to Digital Forensics with work experience utilising cloud solutions within a large financial organisation – preparation as an informed investigator has foundation. Furthermore, access to resources through contacts in the organisation, membership of professional groups and social media associations allow access for further resources with relevant skillset and experience.

Applying these factors and utilising a suitability matrix demonstrating personal and academic validity was adopted to provide overall suitability score. The full dataset of this matrix is found under Appendix II however in summary, the topic specifically around cloud computing and digital forensics scored more favourably than other topics considered such as the law aspect alone.

An opportunity to research and potentially contribute to debate has appeal and relevance to stakeholders such as cloud providers/users, academics, law enforcement agencies and judicial government institutions. A brief stakeholder analysis to determine level of power/interest (Newcombe, 2003) is illustrated below:

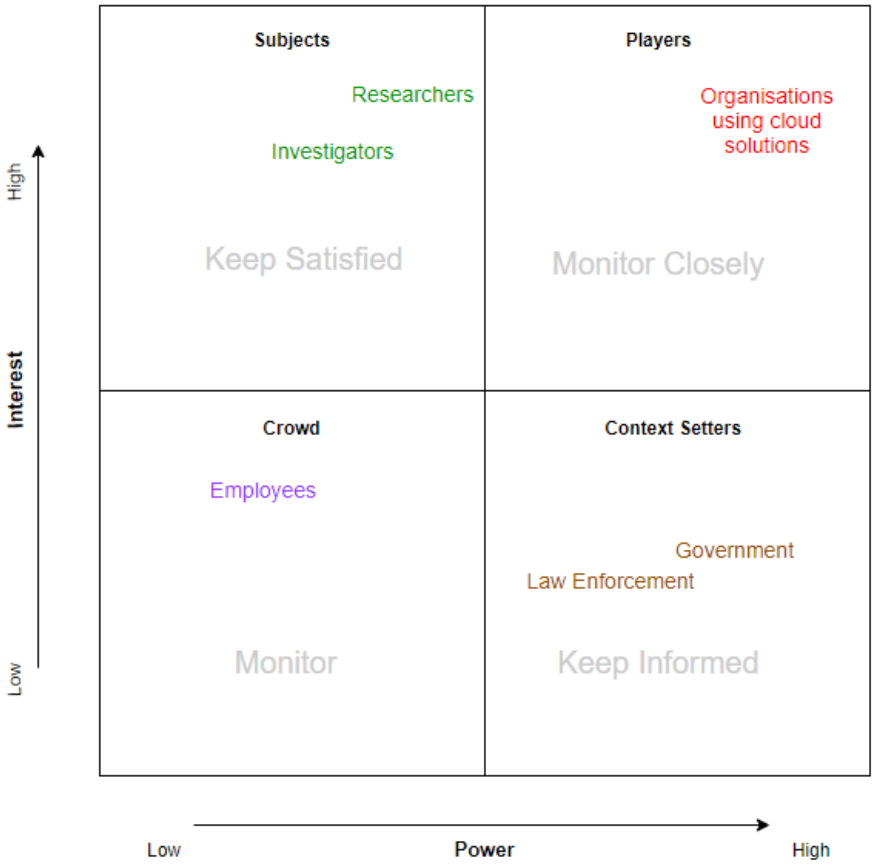

Figure 3: Stakeholder analysis in relation to power/interest in cloud computing and digital forensic impact (adapted from Newcombe, 2003).

The analysis (Figure 3) from a viewpoint of the project, organisations using cloud solutions are of high interest and trends are to be observed. Researchers currently has high interest but not as much influence. Government and Law Enforcement have legislative authority and can influence practices that meet requirements.

2.2 Feasibility

The ideas reviewed in the background relate to the discipline and field of digital forensics. The topic links the challenges, gaps and the effectiveness of proposed frameworks.

The type of research to collect and analyse data is through Primary Research by interviews within the organisation and surveys out to practitioners in the field. The goal of the Primary Research is to explore data directly attained to analyse the challenges posed by forensics within cloud computing and whether newly proposed guidelines are useful in response.

The overall aim of the project is to investigate challenges cloud computing introduces that may hinder successful implementation of digital forensics and whether current ACPO principles are consequently fit for purpose. Meeting the below objectives aid this goal:

- Investigate the current challenges of digital forensics within the cloud
- Determine whether current ACPO principles are fit for purpose
- Undertake an investigation into the 8 principles proposed by Horsman (2020)
- Involve current organisation utilising cloud solutions and practitioners with relevant background on their feedback.

The outcomes of these aims and objectives contribute to debates in the field and arguably a lack of standardised frameworks within cloud forensics. Additionally, the objectives meet personal goals in a field of interest. Finally, outcomes for stakeholders provide an insight into challenges faced and potentially updated guidelines.

A feasibility analysis has been used to aid the scale and scope of the project. In order to remain realistic, interview data collection is limited to my current organisation. The interviews are based on survey responses from a wide range of practitioners and experienced professionals in the field. The interview data therefore can be applicable to organisations in general given conclusions triangulated from both survey and interview data.

2.3 Risk

Political issues are naturally involved when taking into consideration any form of law enforcement ultimately headed up by governments. The literature review identified multi-jurisdictional issues that cloud computing introduces which can cause concern for investigators. Examples of current frameworks that can influence direction particularly in public sector include UK government department National Cyber Security Centre which issues the Cyber Essentials framework. This framework however may be rendered irrelevant in other jurisdictions. This is reflected and observed as a challenge itself with reference to jurisdictional reach of local government policies.

Furthermore, the stakeholder analysis previously presented identified governments as a stakeholder having a high power of influence in direction. Ensuring government guidelines or frameworks are therefore acknowledged within research to ensure analysis is both legal and valid.

Ethically, confidentiality and unauthorised disclosure are prominent aspects of many organisations, particularly around information security. An understanding and agreement in how to handle these concepts was made with the organisation in advance to avoid any conflicts or unauthorised use of data.

A Failure model and effects form risk analysis has been performed and provided under the Appendix II that covers all stages of the project. This has aided the breakdown of where the risks are, the likelihood, cause and prevention plan. From this output, identifying high risk areas such as the undertaking of research and final write up that led to investing into further areas of mitigating. Mitigating steps were taken on high-risk areas include early engagement, ensuring enough time given for participants to respond to surveys and keeping a running commentary to ensure an accurate transition to final write-ups.

3. Research Process

The aim of the research is to determine challenges cloud computing introduces to forensic capability. Additionally, the research explores whether ACPO standard practices are sufficient in addressing these challenges.

To meet the aims and objectives the following research questions are proposed.

RQ1 – What are the current challenges of Digital Forensics within the Cloud?

RQ2 – Are the current Association Chief Police Officers (APCO) guidelines sufficient in ensuring the collection of evidence within the cloud?

RQ3 – How effective would the principles proposed by Horsman (2020) be in addressing the challenges of cloud forensics?

The benefits of deploying Research Questions are to provide focus and a clear unambiguous approach to addressing the research aims (Open University, 2012a). Research questions also relate the purpose of the research to its objectives and the output from this method help determine the what and why of what needs to be known (Lipowski, 2008). Lipowski (2008) argues that the development of good research questions forms the most important part of the research process. The critical nature of creating the right form of questions that deliver the aim of the project includes questions that are interesting, engaging and non-ambiguous (Lipowski, 2008).

There are particular risks associated with deploying research questions as a core process for research. Lipowski (2008) provides an example that there is little guidance about the generation of development of good questions. It can therefore be derived that good or valuable answers rely heavily on good questions. Furthermore, Goldschmidt and Matthews (2022) suggests that it is conceivable that even if research questions are well crafted and justified, it may yet struggle to make a significant contribution potentially leading to newly generated questions for further study.

Goldschmidt and Matthews (2022), however, accepts the value of deploying research questions towards research areas of phenomena interest and underdeveloped areas that are engaged in debate which the literature review from Section 1 demonstrates.

3.1 Causality

The model of causality informing the research is through the Context, Mechanism and Output (CMO) model which aims to provide causative explanations from observed data (Jagosh *et al.*, 2014). This fits in with the research approach taking the *mechanism* of digital forensics in the *context* of cloud computing and the consequent challenges and mitigations as the *outcome*. While this is a simplistic interpretation, it assists the categorisation of the CMO model in both delivering the aims and designing the research effectively. Understanding these interactions between the mechanisms and context is crucial to analysing outcomes correctly (Falleti and Lynch, 2009). It is therefore not a linear approach nor cause and effect.

Ultimately, the successful outcome of the CMO approach is determining what works under which circumstances (De Souza, 2013). The potential drawbacks of the CMO approach are the potential conceptual challenges that is time consuming (De Souza, 2013) which was a risk to the time constraints of the project.

3.2 Research Paradigm

The research paradigm applied is the Naturalistic research approach. This is in contrast to traditional scientific/positivist methodology and instead, naturalist research results in more multiple truths based on subjective experiences (Open University, 2012b). While naturalistic research has roots in Social Sciences (Open University, 2012b) and used extensively by zoologists and naturalists (Salkind, 2010), the concepts are equally applied to this project by observing and recording outputs from answering research questions.

Comparing both interpretivist or constructivist approaches within Naturalistic methodology has implications on applicability of results. The constructivist approach aims to generate new knowledge creating clear accounts in comparison to interpretivist where outcomes are relative open to authentic representation (Open University, 2012b). Interpretivism therefore allows generalisation of results compatible with the use of research questions.

As the research process utilises the concept of research questions, rather than hypothesis, the non-experimental aspect of this method makes the naturalistic approach compatible with the research process. The output research has differing opinions, e.g., multiple truths, rather than a repeatable experiment testing a hypothesis. This makes the naturalistic approach having more congruency with the aims and research questions of the project. The design of the questions takes an interpretivist approach to allow its applicability in the general field.

While the scope is cloud computing, demonstrating objectivity analysing challenges and frameworks by questioning future challenges within digital forensics outside the cloud is included to prevent assumptions that only cloud computing present challenges and applicability of any proposed frameworks.

3.3 Research Methodology

Primary research is the preferred approach where data is newly collected and analysed, also known as empirical research as it's based on direct observation (Open University, 2012c). The empirical research method would be inductive, where observations are made around a phenomena of interest to form concepts or theories (Woiceshyn and Daellenbach, 2018). This is in line with the Naturalistic approach analysing observations from research questions posed. This is contrast to the deductive approach where deriving a hypothesis, testing it and deducting whether the theory requires revision (Woiceshyn and Daellenbach, 2018).

The overall approach taken is a mixed method approach collecting both quantitative and qualitative data through surveys and interviews respectively. One of the aims of the project is identifying challenges of digital forensics processes within cloud computing and whether relevant mitigating frameworks in place. The quantitative data from surveys aims to identify trends and gauge opinion on challenges with qualitative data probing deeper into Horsman's (2020) principles.

The combination of survey and interview methods drives the analysis of data to conclusion. The quantitative aspect establishes themes and weight in numbers identifying the challenges and qualifying trends through interviews.

The benefits of triangulating the analysis of data provides the following benefits (Somekh and Lewin, 2004)

- Increased understanding with strong credibility and validity
- A more complete formation of analysis from multiple perspectives
- Deeper insights potentially requiring reconciliation with further research
- Greater diversity of values through the inclusion of mixed methods

Somekh and Lewins (2004) observations on the benefits of combining quantitative and qualitative analysis provides depth and credibility in the presentation of collected data. Ensuring the qualitative data is relevant and robust, the quantitative outputs from the themes of the challenges and current framework suitability can be used to drive the qualitative aspect of the research and feed into its design. This is the justification applying both Survey and Interview methods together providing the depth, credence and fluidity to drive Interviews based on Survey observations.

Therefore, ensuring the approach to attaining valuable and objective quantitative and qualitative data is crucial. To structure this, thematic analysis (Braun and Clarke, 2006) is applied. Braune and Clarke (2006) proposes six phases to prepare the implementation of thematic analysis:

- Data familiarizing
- Generating initial codes
- Theme searching
- Theme reviewing
- Defining and theme naming
- Report producing

Section 1.1 laid the background and current debate around cloud forensics phenomena. Themes from literature aid the identification of potential patterns from the data collection. Therefore, the literature review provides the basis for validating and investigating themes using thematic analysis. It is these 6 steps from Braun and Clarke (2006) being applied to interpret results and answer the research questions.

3.4 Methodology Discussion

The applicability of adopting a naturalistic paradigm combining the quantitative and qualitative analysis provides suitability of the nature of research design. The flexibility and less formal planning naturalistic research (Salkind, 2010) allows the research to remain fluid within time constraints. In contrast, a positivist approach requires a specific theory and a hypothesis to be tested against (Open University, 2012d). Therefore, repeatability, predictions and proof associated with positivist approaches (Open University, 2012d) isn't compatible with multiple variables within this project. This results in predicting a hypothesis problematic.

The data collection through surveys and interviews aided the analysis in the following ways:

- Quantitative data from the survey informs the qualitative research through interviews, e.g., identifying themes and trends to be explored further.
- Data informs a report output answering the research questions posed by reconciling data from quantitative and qualitative sources.

The risk applying a combination of quantitative and qualitative methods is the potential process of iteration due to the variables in place. However, applying a thematic mindset (Braun and Clarke, 2006) mitigated and structured qualitative data.

The literature review from Section 1 demonstrates a wide-ranging debate without a standout framework for cloud forensics and hence secondary research poses difficulty in drawing conclusions or satisfactorily answer the posed research questions. As the research is aimed to be applicable generally, a case-study approach limits a convincing narrative.

3.5 Data Generation/Collection Methods

The data collection method in conducting the research was surveys through questionnaires and interviews. The term survey, which can be defined as a procedure where information is systematically collected from a defined population where conclusions can be reached from this population (Thomas, 1996).

3.5.1 Questionnaires

The themes and challenges derived from the literature review from section 1 formed the basis of the design of the questionnaire.

Ponto (2015) observes the use of surveys has been in place for decades and obtaining information relatively quicky and the extraction of questionnaire data from the 25 participants for this research has been experienced. In order to address the research questions effectively and filling in gaps the use of both ranking items as well as open ended questions were employed. This is consistent with the mixed-approach to the research methodology and practicality of the time constraints on the project.

The importance of participants having the right background and experience is crucial and have been targeted to include those to have a background in IT or clouding computing. These participants have been identified through contacts within the organisation, professional bodies, relevant social media groups within cyber security and LinkedIn. This participant profiles are reflected through the demographic's subset of questionnaire data.

The eight proposed principles from Horsman (2020) formed a key part in critically analysing claims, and while not all eight are asked in the survey, the first principle is included to determine an initial trend to feed into divulging deeper into interview stages later to discover if trends reconcile across all eight principles. This was to keep the questionnaire engaging and interesting which is measure of good design of questioning (Lipowski, 2008) hence it was not practical to explicitly ask about all eight

Horsman principles through the survey. Further claims made by Findlay (2020) on the need to adapt inspires the inclusion of an open-ended question to determine whether participants are aware of any updated frameworks and specify if so.

In summary, the questionnaire as shown in Appendix III was designed to identify challenges themes and whether respondents agree with findings from the literature review in Section 1. Having a combination of rank type questions as well as qualitative open-ended questions is analysed and shape the interview questions and the data is reconciled between both forms of data collection.

3.5.2 Interviews

The data and trends observed from the questionnaire drove the focus of the interview questions, in particular themes and framework subject areas that have overall rankings or specified outputs from open ended questions. To compliment the questionnaire effectively, a semi structured approach probing the responses where applicable (Open University, 2012e) particularly when detail was offered from questions. Interviews are normally classified as qualitative forms of data (Halcomb and Davidson, 2006) and while disadvantages may be responses may not be comparable they will contribute to answering the research questions. Applying thematic analysis mitigated this disadvantage.

Halcomb and Davidson (2006) argues that a fully structured interview takes a quantitative approach and hence the semi structure and even an informal conversation keeps the outcome of the data gathered from interviews qualitative in nature.

Reconciling both quantitative and qualitative data from the questionnaire and interviews was analysed identifying whether themes or challenges from literature review were upheld. Furthermore, the analysis added further credit or discredit Horsman's (2020) and Findlay (2021) observations on the suitability of the current ACPO frameworks in the context of cloud computing from the responses asking this question directly.

The target sample for interviewees are a selection of employees within my organisation within cyber security and business operations. After a pilot interview it was deemed beneficial for interviewees participate in questionnaire which following interviewees did. To mitigate potential conflicts of interest, no direct team member where authority or influence existed had participated.

Ensuring the effectiveness and the capturing of fluid data that interviews brought, the proposed process stated by Halcomb and Davidson (2006) was planned and consistent with previously stated research methodology. This was subject to recordings having explicit permission.

1. Audio recording of interview with note taking
2. Reflection immediately post interview
3. Listening to recording and amending notes accordingly
4. Preliminary content analysis
5. Secondary content analysis
6. Thematic review

Table 3: Data Management steps: Halcomb and Davidson (2006)

3.5.3 Collection Methods Discussion

While surveys and their forms have proven to be an invaluable form of data collection (Ponto, 2015), they have some weaknesses. These include margins of error from both the researcher and participants perspective. From a researcher perspective, the quality of answers is only as good as the quality of the questions posed and for a participant, there is the possibility of non-truthful answers. Having the surveys tested, user friendly and following best practices defined by Lipowski (2008) helped mitigate as well as a large dataset reducing the margin.

A method that has been dismissed from the outset is the experimental approach that determines cause and effect (Open University, 2012g). The approach is incompatible with efficiently extracting the required data to answer the research questions that are not necessarily repeatable or tested by hypothesis.

In order to mitigate these weaknesses, a pilot approach for a trial launch of the questionnaire was taken to ensure level of engagement and interest were maintained. Feedback was also attained to ensure the flow questions were understood and answered accurately. Similarly, although there were no pilot participants for interviews, the first interview was used to reflect more on responses and identify areas that were not as clear and be improved upon.

Appendix III/IV provides questionnaire and sample interview questions. Ensuring interviews are prepared and better informed, the questionnaire survey was issued and reviewed before conducting interviews. Microsoft Forms, the chosen method of deployment, aids the analysis organising the demographic of participants, e.g., qualifications/experience and consequent opinions on cloud challenges and suitability of frameworks.

4. Data Collection & Analysis

4.1 Data Collection and Generation Report

The data collection and generation method for the research were based on the approach of questionnaires and interviews. The questionnaire was distributed via contacts within my organisation and relevant LinkedIn groups that have members associated or qualified in cloud computing. The questionnaire was eventually extended to other social media platforms such as cyber security groups in Facebook which had members within it whom are professionals in the field to push for extra responses. These steps taken were to maintain the quality of data being collected.

Before wider distribution of the questionnaire, an initial selection of participants from my organisation were asked to pilot the questionnaire to attain feedback from a respondent's perspective in case of any adjustments required. The feedback from pilot users was positive and found the questions engaging as well as thought-provoking and showed interest in the results of the research when they become available. There was no feedback on questions that were found to be difficult or misunderstood.

The questionnaire delivered the quantitative data providing the basis of discussion in interviews providing more qualitative data. In particular, further exploration of the 8 Horsman principles was planned if responses to the questionnaire showing a trend of a positive benefit of the 1 principle included in the questionnaire. The booking of interviews was taking place in parallel of the distribution of questionnaires but scheduled for late February to allow the responses of questionnaires to help define areas of focus or further opinion. All interviews planned were participants from my organisation with a 50-50 split of a technical and an operations/business background.

4.1.2 Data Collection Discussion

After an initial influx of questionnaires being received, it reached a peak from which a further push and reminders were sent. This is to maximise the ability to identify trends and themes which allowed the number of responses to reach 25 in total which was deemed acceptable. Additionally, further groups within Facebook that had professionals within cloud computing were identified and targeted as part of the initiative to seek further responses.

In order to prevent any slippage of already tight time constraints and allow for interviews to take place as scheduled with busy participants, statistical data from questionnaires were analysed in a descriptive manner to make up for a potential shortfall of a significant quantitative set of data. The final number of responses were used to analyse themes and trends as well as contributing to interview questions.

A higher-than-expected response in free text optional forms where it was requested for any other challenges within forensics in cloud computing in addition to the 6 challenges asked was welcome as this provides emphasis on further challenges and could be the basis of future research or discussion in interviews.

For the interview participants, in order not to risk the validity and reliability of data and avoid a 1-dimensional nature of data for analysis, it was important to maintain the requirement of having perspective from both a business and technical background. Ensuring a 50/50 distribution a total number of 4 participants were selected with 2 from business/operations and remaining 2 from technical backgrounds. This resulted in having a total of 4 interviews, slightly below the 6-8 target however having an even distribution of qualitative data from a range of backgrounds mitigates the slight shortfall and utilise time effectively.

4.2 Analysis and Findings

To aid analysis of the data collection and generation, the approach implemented can be summarised into the following 3 categories:

- Built in tools available within Microsoft Forms
- Descriptive Statistical Analysis
- Thematic Analysis

A benefit of Microsoft Forms, in addition to the creation of the questionnaire and ease of distribution, is the ability to summarise the data provided and organise them in charts, average scores, rankings and provide a full extract of the raw data for manual analysis. The automation of these features provides from the offset and throughout the duration of the survey a well-presented summary of results to aid with analysis.

The data provided from raw survey data can be further analysed by using descriptive statistical analysis. This technique can be applied to organise, present and analyse data (Fisher and Marshall, 2009). The use of descriptive statistics provide a method of allowing research outcomes based on evidence, give insight and summarise quantitative data (Marshall and Jonker, 2010).

Specifically, the use of common terms used in descriptive statistical analysis can be summarised by the table below. These terms contribute to the techniques applied to present research findings with rigour and assimilated easily by readers as well as meaningful contribution to research questions (Marshall and Jonker, 2010).

Term	Definition
Mode	The numerical value with the greatest frequency
Medial	The middle score of a rank ordered distribution
Mean	The average score

Table 4: Common statistical terms and definitions (Fisher and Marshall, 2009)

While descriptive statistical analysis is applied for more quantitative or survey data, it is less useful for more qualitative data gathered from interviews. This is where thematic analysis is applied and the justification of taking this approach are both the inadequacy of common statistics such as median/mode and consequently a systematic approach is taken for qualitative data.

The 6 steps for thematic analysis (Braun and Clarke, 2006) is applied to interpret results contributing to answering research questions. The simplification comes from theme searching that produces outcomes based on recurrences of themes identified.

Mixing these tools and techniques together contribute to the efficient, simplification and combined contributions of summarised data to answer the research questions posed.

4.2.1 Questionnaire Findings

4.2.1.1 Demographics

The demographics of participants of the research from practitioners and professionals in the field ensures rigour with valuable contributions opinion to the phenomena. The demographic data can therefore demonstrate the appropriateness of participants used for the study (Connelly, 2013).

The demographics for survey data was focussing on years of experience in IT, association with cloud computing, cloud certification and awareness of ACPO principles.

The first six questions of the questionnaire shown in the Appendix III are dedicated to demographic data. A sample of these findings are summarised below.

Question 1: How many years of experience do you have in the field of IT?

Figure 4: Responses to years of experience participants have in IT.

Question 3: Do you have experience (past or present) working with some form of cloud computing?

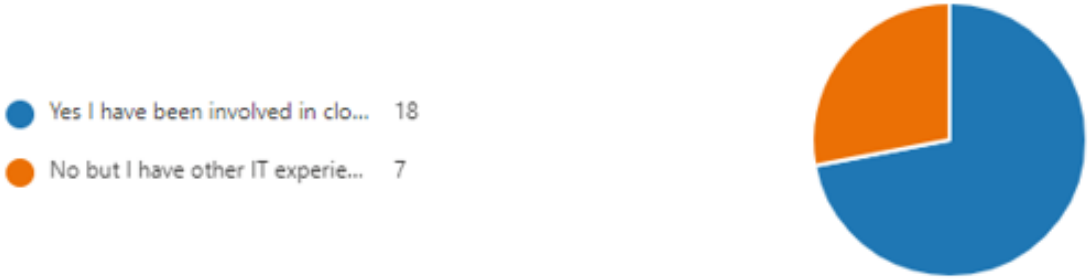

Figure 5: Responses to past or present experience working with a form of cloud computing.

Question 4: Do you currently hold any professional certifications in the field of Cloud Computing?

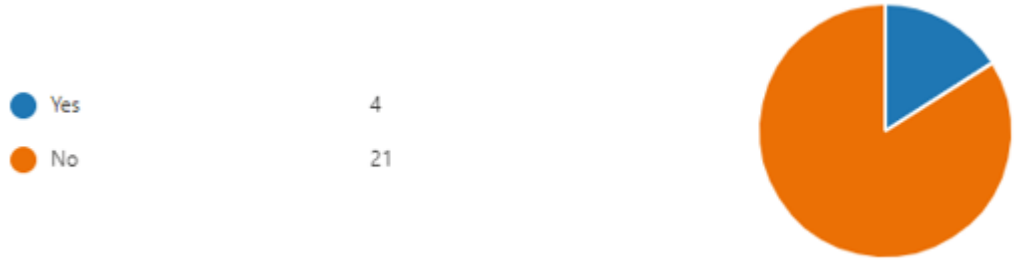

Figure 6: Responses on whether participants hold any professional certifications in Cloud Computing

Question 6: Are you aware of the 4 principles defined by the Association of Chief Police Officers (ACPO) for digital forensic evidence processing?

Figure 7: Responses on participants awareness of ACPO principles

The majority of participants from this data show the majority have 10 or more years' experience in IT (Figure 4), with exposure of cloud solutions (Figure 5) and a majority of having at least vague awareness of the ACPO principles (Figure 7). A further number of 4 held professional qualifications in cloud computing (Figure 6). The profile of the demographic's correlates to the targeted audience of practitioners in the field with experience of cloud and forensic backgrounds.

4.2.1.2 ACPO & Challenges

The next section gauges opinion on whether ACPO principles are fit for purpose and the challenges that exist to perform forensics within the cloud environment.

Question 7: Do you believe the current ACPO guidelines are sufficient for processing digital evidence within the Cloud?

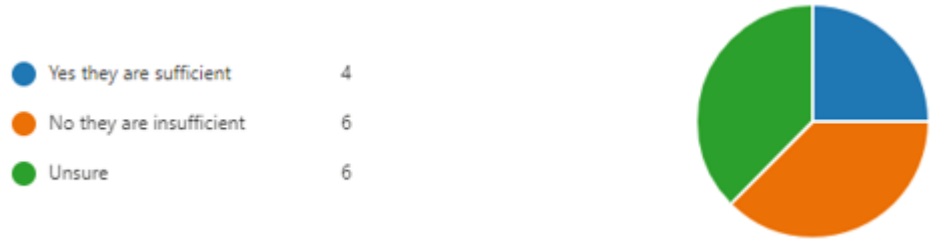

Figure 8: Responses on participants belief on ACPO sufficiency

Only participants whom had at least vague awareness of ACPO (Figure 7), were presented with the question in Figure 8 as without any awareness of ACPO answering on its sufficiency potentially

endangers informed opinion. Ensuring those who had some awareness of ACPO allowed them to make a more qualified assessment in ACPO sufficiency. A significant portion are at least unsure or state that current ACPO guideless are insufficient.

Furthermore, the first principle proposed by Horsman (2020) was presented to respondents to investigate whether this should be considered as part updated principles.

Question 19: Please review the below proposed principle by Horsman (2020).

"All extracted and interpreted data deemed to be 'digital evidence' must have undergone robust testing and validation using accepted testing methods and peer review in order to verify accuracy"

Do you feel this is necessary to be mandated for inclusion in a standardized guideline framework for processing digital forensic data?

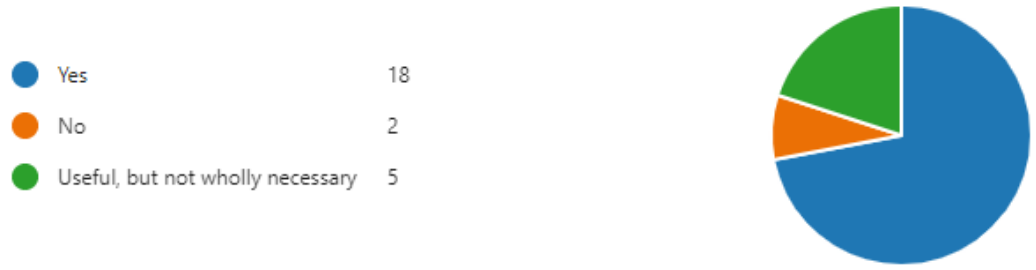

Figure 9: Responses on participants view on inclusion of Horsman (2020) principle 1 in future frameworks

Out of 25 respondents, only 2 felt this would not be useful (Figure 9). This provided impetus to explore further in interviews whether the remaining 7 Horsman principles would benefit being included in ACPO guidelines in response to challenges posed by cloud computing.

Six challenges are then presented to all participants and were asked to score on a scale of 1-10 (with 10 being most challenging) that each scenario presents. The mean score from all challenges is then calculated which resulted in the below table ranking of most challenging scenarios:

Rank	Challenge	Mean Score
1	Multi-jurisdictional challenges Cloud environment forensics.	7.48
2	Evidence gathering from cloud environments can ensure integrity without contamination of data.	6.8
3	The integrity of the chain of custody is preserved within Cloud environments.	6.76
4	Relying on Cloud Service Provider to aid forensics processes by providing the identification, preservation and ability to collect any evidence.	6.4
5	Cloud's ability to access and provide relevant data to aid a forensic or audit investigation.	6.0
6	Cloud environment's ability in collecting logs to aid a forensic or audit investigation.	5.4

Table 5: Challenges of cloud forensics ranked by participants

The highest scoring challenge echoes sentiments from literature commentary on multi-jurisdictional issues (Daryabar et al., 2013; Morioka and Sharbaf, 2016) and highlights a non-technical challenge hindering processing of forensic cloud evidence. Similarly, ensuring the integrity and chain of custody of evidence trends highly and potentially confronts the suitability of current ACPO applicability in the cloud where integrity without contamination and chain of custody is paramount.

Additionally, optional commentary from participants (Appendix III) in this section expanded on jurisdictional issues providing further emphasis, samples of such commentary are below.

"*Previous cases involving the likes of Apple/Amazon/Google/Facebook have demonstrated how reluctant the corporations are to provide access to such data, beyond purely sovereign jurisdiction over where data is stored*"

"International or regional/ state-based law and GDPR are biggest obstacle"

"Cloud computing is complicated because of the multitenant nature of systems……..and trust in institutions to comply with requests"

The following question explores the 3 categories of challenges and participants were asked to rank these in order with 1 (top) being the highest impact. The data was observed using Mode analysis of the highest frequency top-ranking category:

Question 15 - Please rank in order, 1 (top) being the highest impact, the following categories that introduces the biggest challenge for cloud forensic functionality that would need most attention:

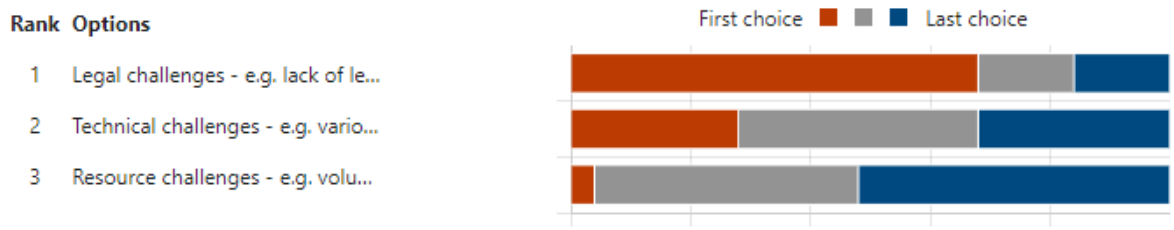

Figure 10: Participants ranking of challenge categories

With technical and resource challenges scoring second and third respectively, responses identify an emergence that the most challenging aspect cloud computing introduces are legal complications including the lack of legislation and jurisdictional differences (Figure 10). While Al Fahdi, Clarke and Furnells (2013) summarises these challenge types, it does not ascertain which category is most pressing stating no studies on opinions and attitudes towards these challenges were performed. This result contributes to this gap in opinion.

4.2.1.3 Current Frameworks & Future Challenges

Given the expansion of organisation using cloud computing solutions, the below question prompts participants awareness of any standard practices to apply such solutions.

Question 17 - Are you aware of a standardized framework for Cloud Computing forensic practices?

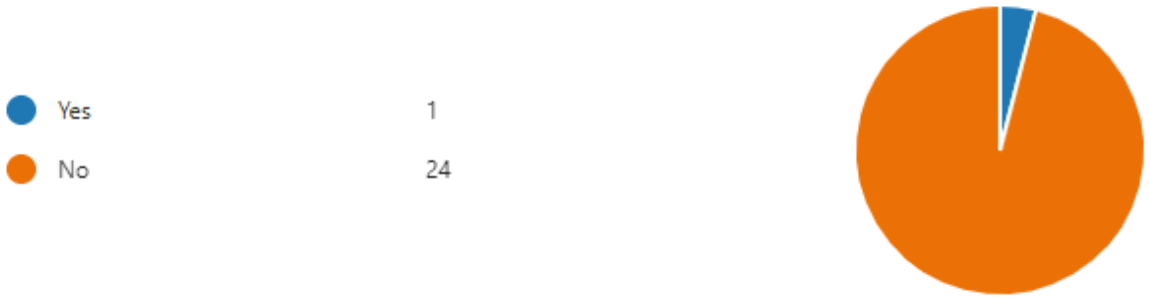

Figure 11: Participant's awareness of standardized frameworks for cloud forensics

24 out of 25 states they were not aware of any standardized framework for cloud computing and the 1 participant that stated yes gave a free text response of "MI5" which is not a standard framework. This suggests despite the growth of cloud computing and potential challenges, there is not a widely known standard framework to apply its implementation.

The future outlook based on future challenges from literature gave an insight on participants view on future challenges for digital forensic processes.

Question 20: Please rank (1 highest - 9 lowest) from the below list whether these pose challenges in the future for Digital Forensic processes.

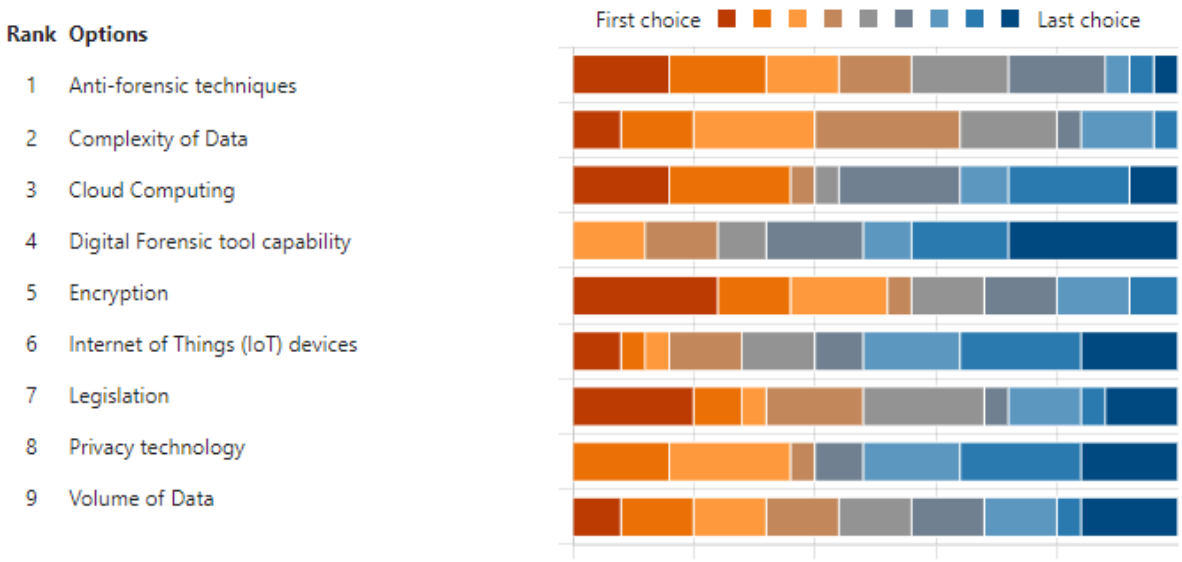

Figure 12: Participants rankings for future challenges in digital forensics

The expected challenges of Legislation and Cloud computing remain scoring highly for future challenges suggesting it could be a long-term issue. Encryption, Anti-forensic techniques and complexity of data make the remaining of the top rankings adding considerations for potential future practices to mitigate these challenges.

4.2.2 Thematic Analysis of Interviews

4.2.2.1 ACPO Suitability

In order to compliment quantitative data from the survey, the interviews conducted probe deeper, in particular, to Horsman's (2020) argument of ACPO requiring an update following the growing use of cloud computing and digital evidence.

Figure 9 from questionnaire data which presented principle 1 of Horsman's (2020) proposal gave a positive response for inclusion in future frameworks for cloud forensics. This and the 7 remaining principles were a focus of the interview and in particular keywords from literature (Al Fahdi, Clarke and Furnell, 2013; Irons and Lallie, 2014; Horsman, 2020; Findlay, 2021) such as suitability, relevance, complexity, resources and inclusion were noted to identify themes. This is part of the thematic analysis to identify codes aiding the process. The transcript was also reviewed iteratively to identify further keywords that emerged from responses and were coded accordingly.

After brief introductions on background, interviewees were asked on opinions on suitability of current ACPO guidelines and their suitability in ensuring digital evidence. Varied responses of opinion were observed to this question and to a certain extent correlates to question 7 from the survey (Figure 8). A summary of these responses is noted below.

Interviewee	Background	ACPO fit for purpose	Opinion
1	Technical	N	ACPO has not adapted to fast moving changes in industry such as cloud or Internet of Things. These changes warrant a refresh of ACPO.
2	Technical	Y	The generic nature of ACPO simplifies the complexities of gathering digital evidence and can be counter-productive if changed resulting in potential court cases being dismissed on technicalities
3	Operations	N	Advised ironic guidelines are static in comparison to rapidly developing technologies
4	Operations	N/A	Advised not qualified to comment

Table 6: Interviewees opinions on ACPO suitability

The range of opinions to this debated question is varied and the following analysis can be derived from these:

- Current APCO Principles are sufficient to keep guidance simple giving best chance of producing forensic evidence being accepted in court.

- Current APCO Principles are insufficient due to change in technological advances since the inception of the original guidelines more than a decade ago.

4.2.2.2 The 8 Horsman Principles

Each of the interviewees were presented printouts of the 8 proposed principles of Horsman (2020) (Appendix I) and read in turn asking about suitability of inclusion in an updated version of ACPO. To present the outcome of this data thematically, a table summarising whether each principle should be included (Yes/No/Unsure) and associated keywords observed on each answer are tallied. The keywords emerged from transcripts were summarised into codes below:

Code	Theme	Description
C	Complex/Complicated/Unrealistic	Negativity due to complications or complexity from principle
I	Irrelevant / Not Needed	Negativity due to irrelevance of principle
S	Suitable	Positivity due to benefits of principle
E	Essential	Positivity stressing relevance and benefits of principle
V	Volumes	Negativity due to lack of resources or large volumes of data

Table 7: Thematic code summary

Combining all responses on the Yes/No question on whether each principle should be included and associated justification is tallied by thematic codes. The results from this data are summarised below.

Horsman Principle	Inclusion Y/N/Unsure (Interviewee 1/2/3/4)	Codes	Score (Green +1 Red -1 Unsure 0)
1	Y N Y U	I E E S S C	3
2	N N Y Y	I E C C S S E C V	-1
3	Y U Y U	S C C C S C C	-1
4	Y Y Y Y	E S S C S	7
5	N Y Y Y	I E S S V	3
6	Y Y Y Y	E E S E V C	6
7	N Y N U	C C I E S V V	-4
8	Y Y Y Y	E S S S	8

Table 8: Thematic analysis summary of interview respondents based on Y/N inclusion and codes from Table 7

The summary from interviewee opinion scores Horsman (2020) principles 4,6 and 8 more favourably and in contrast 2,3 and 7 least favourable. Complexity of the principles recur frequently in much of the feedback with the exception of principle 8. Even where interviewees identified positivity for inclusion, complexity was still highlighted as shown on feedback for principle 4. A possible explanation on the contradiction of being favourable for inclusion and highlighting complexity can be summarised by the below transcript from interviewee 1 (Appendix IV):

> *"While all these proposed principles are suitable in nature and certainly beneficial, in the real world to consistently achieve all 8 is not only complicated but unsustainable in an ever-growing dataset across wide ranging devices can place huge burden on those performing the work"*

Complexity as a theme may be emerging but Interviewee 3 commented that this is a reflection of where technology stands today (Appendix IV):

> *"Similar to the way technology advances and in turn cyber criminals look for ways to exploit – ACPO must at least reflect and mitigate any gaps created by advances to ensure the integrity and inclusion of digital evidence in today's world".*

The complexity of the principles are most likely due to the complex nature of cloud computing challenges as outlined in literature from (Chen *et al.*, 2019; Jain and Mahalkari, 2019; Montasari and Hill, 2019).

Based on the highest and lowest scoring, it can be surmised that principle 8 is most favourable for inclusion and principle 7 least.

5. CONCLUSION

Referring back to the quote from Brodkin, J (2008) in section 1.1 on cloud computing investigation difficulties, it can be argued that this still has some relevance today. The long ranging debate in academic literature (Zargari and Benford, 2012; Rani and Sravani, 2016; Choo, Esposito and Castiglione, 2017; Jain and Mahalkari, 2019) along with responses collected from primary data sources demonstrate the complexities, challenges and standardization issues that contribute to cloud forensics.

The below research questions were proposed to meet the aims and objectives:

RQ1 – What are the current challenges of Digital Forensics within the Cloud?

RQ2 – Are the current Association Chief Police Officers (APCO) guidelines sufficient in ensuring the collection of evidence within the cloud?

RQ3 – How effective would the principles proposed by Horsman (2020) be in addressing the challenges of cloud forensics?

5.1 RQ1

The introduction and growth of cloud computing has disrupted and caused debate within academia as demonstrated in section 1.2. Categorising the 3 types of challenges is summarised below:

Challenge Type	Examples
Technical	Different media formats; encryption; anti-forensics; analysis
Legal	Jurisdictional issues; lack of standardised international legislation
Resource	Volume of data; time taken to acquire and analyse

Table 9: Al Fahdi, Clarke and Furnells (2013) – challenge types within cloud digital forensics

Secondary research surmises a persistent debate on the challenges introduced by cloud computing has on digital forensic processes. The sample from 25 practitioners and professionals in the field highlights legal and jurisdictional as obstacles along with the complexity they bring. A dependency is placed on Cloud Service Providers to aid cloud forensic data, maintaining integrity and preservation with further research needed on how effective providers are.

Additionally, multi-tenancy platforms across different geological locations brings further complexity to ensure the integrity of the chain of custody and prevention of contaminated data. This poses an additional non-technical element to the challenges of digital forensics to existing technical requirements. Equally, the requirement of co-operation with third parties to ensure the release of evidence held differs significantly from traditional search and seize methods all within the same crime scene.

5.2 RQ2

Horsman, (2020) argues current ACPO guidelines are not fit for purpose as no significant updates have been made over the last decade despite technological advancements. The data from both questionnaire and survey generally agree with this sentiment.

While not overwhelmingly conclusive, strong arguments back up Horsman's (2020) opinion where the introduction of cloud computing and its challenges potentially renders current frameworks redundant. In balance, a counter argument is that frameworks are designed to be simple and less cumbersome. A lack of standardised cloud forensic practices potentially risks the ability detecting, preserving and processing cloud digital evidence.

5.3 RQ3

Regardless of any argument to update ACPO principles to reflect challenges cloud computing brings to digital forensics, is what can replace it. Horsman's (2020) paper on updating outdated APCO principles has explicitly proposed 8 new principles as an example of bringing digital forensic processes up to date.

The data from the survey and interview although holistically similar, through its qualitative exploration in interviews give context that is less convincing than what initial survey data suggests. The majority of questionnaire participants agreed with a sample principle from Horsman benefits to be included in an updated ACPO framework. Similarly, participant interviewees showed a general positive response to Horsman's principles but crucially this came with caveats. A recurring key word throughout the interview revolves around complexity. It would take work or further research to discredit Horsman's proposal's but can equally be challenged on how these proposed principles complicate the digital forensic gathering process.

As determined from survey data, multi-jurisdictional issues pose a real challenge. Lawyers for example specialise in their own areas of expertise within their own jurisdiction. Would investigators need the requirement to understand law matters across multiple jurisdictions? While Principle 2 does not "place obligation" to understand the full legal landscape it implies the benefits of such attributes.

It can be argued aspects of Horsman's proposals have a case recommending updates to ACPO practices but further research is required to understand the risk of adding too much complexity that can be counter-productive. A compromise of partly including some principles that aid jurisdictional matters may be the best outcome to aid an organisations readiness in response to new challenges introduced by cloud computing. Principles 4 and 8 are potential contenders for this based on interview data.

5.4 Recommendations

The following recommendations as a result of the research can be summarised as follows:

- With cloud computing introducing a multi-tenanted platform across potential different geological locations, organisations must have an understanding of in scope jurisdictions and have legal representation in these areas.

- The Association Chief Police Officers (APCO) guidelines are at risk of being outdated as digital evidence has significantly changed in the last decade with the growth of cloud computing. A review of ACPO is recommended to adapt to this.

- Horsman (2020) proposes a number of principles that are of value but care needs to be taken to avoid complexity and further research is required to determine the delicate balance between complexity and responding to newly created challenges when considering additional principles.

5.5 Conclusion Summary

Cloud computing has disrupted traditional ways digital evidence is produced, the far-reaching data that can be attributed to a single user complicates traditional methods of digital forensics (Neware and Khan, 2018). Current ACPO guidelines that govern best practices should be reviewed in order to fulfil the integrity of digital collection of evidence that maintains admissibility in courts. If guidelines are based on outdated frameworks, this risks the collection of digital evidence correctly in cloud environments that are legally admissible. With further literature searches conducted post completion of the primary research, Horsman's (2020) eight principles remains the closest proposal to update practices.

The complexity introduced by cloud computing through technical, legal and resourcing factors has led to subsequent complications in addressing forensic challenges requiring careful consideration. This is most likely the reason for the long-standing debate to date and while challenges to ACPO from Horsman (2020) are starting to initiate discussion on its flaws backed up by primary data, ACPO remains unchanged. For how long remains to be seen.

REFERENCES

Al Fahdi, M., Clarke, N.L. and Furnell, S.M. (2013) 'Challenges to digital forensics: A survey of researchers amp; practitioners attitudes and opinions', in *2013 Information Security for South Africa*. *2013 Information Security for South Africa*, pp. 1–8. doi:10.1109/ISSA.2013.6641058.

Almulla, S., Iraqi, Y. and Jones, A. (2014) 'A State-Of-The-Art Review of Cloud Forensics', *Journal of Digital Forensics, Security and Law* [Preprint]. doi:10.15394/jdfsl.2014.1190.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. doi:10.1191/1478088706qp063oa.

Chen, Guangxuan *et al.* (2019) 'Research on Digital Forensics Framework for Malicious Behavior in Cloud', in *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 1375–1379. doi:10.1109/IAEAC47372.2019.8997702.

Falleti, T.G. and Lynch, J.F. (2009) 'Context and Causal Mechanisms in Political Analysis', *Comparative Political Studies*, 42(9), pp. 1143–1166. doi:10.1177/0010414009331724.

Fernandes, R. *et al.* (2020) 'A New Era of Digital Forensics in the form of Cloud Forensics: A Review', in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 422–427. doi:10.1109/ICIRCA48905.2020.9182938.

Findlay, B. (2021) 'A forensically-sound methodology for advanced data acquisition from embedded devices at-scene', *Forensic Science International: Reports*, 3, p. 100188. doi:10.1016/j.fsir.2021.100188.

Fisher, M.J. and Marshall, A.P. (2009) 'Understanding descriptive statistics', *Australian Critical Care*, 22(2), pp. 93–97. doi:10.1016/j.aucc.2008.11.003.

Goldschmidt, G. and Matthews, B. (2022) 'Formulating design research questions: A framework', *Design Studies*, 78, p. 101062. doi:10.1016/j.destud.2021.101062.

Guo, H., Jin, B. and Shang, T. (2012) 'Forensic investigations in Cloud environments', in *2012 International Conference on Computer Science and Information Processing (CSIP)*. *2012 International Conference on Computer Science and Information Processing (CSIP)*, pp. 248–251. doi:10.1109/CSIP.2012.6308841.

Halcomb, E.J. and Davidson, P.M. (2006) 'Is verbatim transcription of interview data always necessary?', *Applied Nursing Research*, 19(1), pp. 38–42. doi:10.1016/j.apnr.2005.06.001.

Horsman, G. (2020) 'ACPO principles for digital evidence: Time for an update?', *Forensic Science International: Reports*, 2, p. 100076. doi:10.1016/j.fsir.2020.100076.

Irons, A. and Lallie, H.S. (2014) 'Digital Forensics to Intelligent Forensics', *Future Internet*, 6(3), pp. 584–596. doi:10.3390/fi6030584.

Jagosh, J. *et al.* (2014) 'Critical reflections on realist review: insights from customizing the methodology to the needs of participatory research assessment', *Research Synthesis Methods*, 5(2), pp. 131–141. doi:10.1002/jrsm.1099.

Jain, P. and Mahalkari, A. (2019) 'Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis', *International Journal of Computer Applications*, 178(34), pp. 28–34. doi:10.5120/ijca2019919220.

Lipowski, E.E. (2008) 'Developing great research questions', *American Journal of Health-System Pharmacy*, 65(17), pp. 1667–1670. doi:10.2146/ajhp070276.

Marshall, G. and Jonker, L. (2010) 'An introduction to descriptive statistics: A review and practical guide', *Radiography*, 16(4), pp. e1–e7. doi:10.1016/j.radi.2010.01.001.

Martini, B. and Choo, K.-K.R. (2012) 'An integrated conceptual digital forensic framework for cloud computing', *Digital Investigation*, 9(2), pp. 71–80. doi:10.1016/j.diin.2012.07.001.

Marturana, F., Me, G. and Tacconi, S. (2012) 'A Case Study on Digital Forensics in the Cloud', in *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 111–116. doi:10.1109/CyberC.2012.26.

Miranda Lopez, E., Moon, S.Y. and Park, J.H. (2016) 'Scenario-Based Digital Forensics Challenges in Cloud Computing', *Symmetry*, 8(10), p. 107. doi:10.3390/sym8100107.

Montasari, R. and Hill, R. (2019) 'Next-Generation Digital Forensics: Challenges and Future Paradigms', in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, pp. 205–212. doi:10.1109/ICGS3.2019.8688020.

Morioka, E. and Sharbaf, M.S. (2016) 'Digital forensics research on cloud computing: An investigation of cloud forensics solutions', in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*. *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, pp. 1–6. doi:10.1109/THS.2016.7568909.

'Naturalistic Observation' (2010) in Salkind, N., *Encyclopedia of Research Design*. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. doi:10.4135/9781412961288.n263.

Neware, R. and Khan, A. (2018) 'Cloud Computing Digital Forensic challenges', in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pp. 1090–1092. doi:10.1109/ICECA.2018.8474838.

Newcombe, R. (2003) 'From client to project stakeholders: a stakeholder mapping approach', Construction Management and Economics: A Festschrift for Professor Syd Urry 1925-1999. Taylor & Francis Group, 21(8), pp. 841–848. doi: 10.1080/0144619032000072137.

Open University (2012a) 2.1 Research Questions T847 Weeks 6-9 Block 2 https://learn2.open.ac.uk/mod/oucontent/view.php?id=1757638&printable=1 (Accessed 2nd April 2022)

Open University (2012b) 3.5 Naturalistic research Weeks 6-9 Block 2 https://learn2.open.ac.uk/mod/oucontent/view.php?id=1757638&printable=1 (Accessed 2nd April 2022)

Open University (2012c) 4.1.2 Different kinds of source Weeks 6-9 Block 2 https://learn2.open.ac.uk/mod/oucontent/view.php?id=1757638&printable=1 (Accessed 2nd April 2022)

Open University (2012d) 3.4 Positivist research Weeks 6-9 Block 2 https://learn2.open.ac.uk/mod/oucontent/view.php?id=1757638&printable=1 (Accessed 2nd April 2022)

Open University (2012e) 4.5 Interviews Weeks 6-9 Block 2 https://learn2.open.ac.uk/mod/oucontent/view.php?id=1757638&printable=1 (Accessed 2nd April 2022)

Pătraşcu, A. and Patriciu, V.-V. (2013) 'Beyond digital forensics. A cloud computing perspective over incident response and reporting', in *2013 IEEE 8th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. *2013 IEEE 8th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, pp. 455–460. doi:10.1109/SACI.2013.6609018.

Pătraşcu, A., Velciu, M.-A. and Patriciu, V.V. (2015) 'Cloud computing digital forensics framework for automated anomalies detection', in *2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics*. *2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics*, pp. 505–510. doi:10.1109/SACI.2015.7208257.

Pichan, A., Lazarescu, M. and Soh, S.T. (2015) 'Cloud forensics: Technical challenges, solutions and comparative analysis', *Digital Investigation*, 13, pp. 38–57. doi:10.1016/j.diin.2015.03.002.

Purnaye, P. and Kulkarni, V. (2021) 'A Comprehensive Study of Cloud Forensics', *Archives of Computational Methods in Engineering* [Preprint]. doi:10.1007/s11831-021-09575-w.

Rani, D.R. and Sravani, P.L. (2016) 'Challenges of Digital Forensics in Cloud Computing Environment', *Indian Journal of Science and Technology*, 9(17). doi:10.17485/ijst/2016/v9i17/93051.

Sang, T. (2013) 'A Log Based Approach to Make Digital Forensics Easier on Cloud Computing', in *2013 Third International Conference on Intelligent System Design and Engineering Applications*. *2013 Third International Conference on Intelligent System Design and Engineering Applications*, pp. 91–94. doi:10.1109/ISDEA.2012.29.

Sibiya, G., Venter, H.S. and Fogwill, T. (2012) *Digital forensic framework for a cloud environment*. International Information Management Corporation (IIMC). Available at: https://researchspace.csir.co.za/dspace/handle/10204/5890 (Accessed: 3 December 2021).

Somekh, B. and Lewin, C. (2004) *Research Methods in the Social Sciences*. SAGE.

Vu, K., Hartley, K. and Kankanhalli, A. (2020) 'Predictors of cloud computing adoption: A cross-country study', *Telematics and Informatics*, 52, p. 101426. doi:10.1016/j.tele.2020.101426.

Woiceshyn, J. and Daellenbach, U. (2018) 'Evaluating inductive vs deductive research in management studies: Implications for authors, editors, and reviewers', *Qualitative Research in Organizations and Management: An International Journal*, 13(2), pp. 183–195. doi:10.1108/QROM-06-2017-1538.

Zargari, S. and Benford, D. (2012) 'Cloud Forensics: Concepts, Issues, and Challenges', in *2012 Third International Conference on Emerging Intelligent Data and Web Technologies*. *2012 Third International Conference on Emerging Intelligent Data and Web Technologies*, pp. 236–243. doi:10.1109/EIDWT.2012.44.

Zawoad, S. and Hasan, R. (2016) 'Trustworthy Digital Forensics in the Cloud', *Computer*, 49(3), pp. 78–81. doi:10.1109/MC.2016.89.

TEXT REDACTED FOR COPYRIGHT REASONS

APPENDIX I HORSMAN 8 PRINCIPLES

The eight proposed principles in response to aging APCO digital forensic principles that are arguable aged.

Source - Horsman, G. (2020) 'ACPO principles for digital evidence: Time for an update?', *Forensic Science International: Reports*, 2, p. 100076. doi:10.1016/j.fsir.2020.100076.

[redacted]

[redacted]

APPENDIX II SUITABILTIY MATRIX AND RISK ANALYSIS

Project/topic	Personal suitability	Score	Organizational suitability	Score	Subject suitability	Score	Total +	Total -
Cloud Computing	Area of interest with relevant academic/ commercial experience in field.	+++	Trend setter in industry, organisations are currently migrating or contemplating Cloud Computing	++	Considerable literature on cloud computing aspects	+++	14+	/
Cloud Digital Forensics	Interest gained from previous academic experience and opportunity grow and contribute to area	++	Organisations may show interest but can show reluctance to participate in sensitive operations	-	A strong area of debate that is current and engaging	+++	5+	1-
Digital Law	Area of some interest but although relevant not directly related to more technical interests	+	Might be more relevant to stakeholders involved in law enforcement rather than organisations as a whole	-	Directly relevant to the validity of cloud forensics	++	3+	1-

Risk Analysis									
Project Stage/Process	**Potential failure**	**Potential effect(s)**	**SR**	**Potential cause of failure**	**LR**	**PRN**	**Prevention plan**	**PEN**	**RRF**
General	Time constraints	Impact to completing the project	4	Not sticking to project milestones, personal/work issues	3	12	Stick to milestones and where possible, complete earlier to allow for mitigation	0.5	**6**
Preliminary Reading	Literature not relevant/appropriate	Foundations of project weakened	8	Incorrect selection of literature	3	24	Ensure majority of papers are peer reviewed and relevant to topic and discussion	0.9	**21.6**
Problem/topic definition	Scope not clear/specific	Focus of research and project design would not be up to standard	8	Not taking appropriate feedback, insufficient suitability test performed	3	24	Ensure comprehensive suitability test is performed and engage with any feedback around topic definition	0.9	**21.6**
Detailed problem/topic investigation	Scope too small/large	Incompletion of project due to inefficient or too large of scope	7	Insufficient feasibility assessment performed	3	21	Ensure feasibility exercise fully performed and engage is appropriate feedback	0.9	**18.9**

Research design	Insufficient depth to research design	Potential of attaining valuable data for analysis impacted resulting in missed opportunity for valuable findings and recommendations	7	Unaware of relevant tools Lack of understanding of Block 2 materials	4	28	Research questionnaire tools and understanding how to make the design of research go far in terms of meeting aims	0.8	**22.4**
Undertake research	Insufficient responses to research Unwillingness of organisation to share security information	Insufficient responses / lack of time provided by organisation to participate in interviews.	7	Organisational policies preventing disclosure of information	7	49	Early engagement with organisation and establish agreed framework for co-operation. Ensure enough time for practitioners to respond to questionnaires	0.6	**29.4**
Analysis	Inadequate process for analysis	Missing opportunities to derive value of recommendations from analysis	6	Insufficient understanding of data analysis	2	12	Learn and develop techniques for effective data analysis.	0.9	**10.8**
Findings and recommendations	Inadequate result set Unable to derive recommendations	Not contributing significantly to theory/practice or organisational aims in identifying readiness in applying cloud forensics	5	Poorly designed research design	6	30	Establish network early on and understand any challenges from participants that may impede participation in research. Have a social media platform as a backup in case of any issues with targeted participants	0.5	**15**
Writing up	Word count restrictions/valid executive/summary/conclusions	Impact to overall grade if quality of summary,report,findings, conclusions not completed within word limit restrictions	8	Lack of planning	4	32	Ensure continuous planning, keeping an open mind and frequent note taking as you go along. The project may go through multiple edits but its important to keep a form of running commentary along the way to ensure no thinking has been missed. Aggressively keep to timescales and being conscious of milestone deadlines.	0.9	**28.8**

APPENDIX III – QUESTIONNAIRE DATA SET

1.How many years' experience do you have in the field of IT?

Student/Graduate/up to 1 year	0
1 - 3 years	0
3 - 6 years	3
6-10 years	2
10 years+	20

2.Does the organization you work for / associated with (i.e. Workplace or Educational) utilize cloud solutions?

Yes	23
No	1
Unsure	1

3.Do you have experience (past or present) working with some form of cloud computing?

Yes I have been involved in cloud computing	18
No but I have other IT experience	7

4.Do you currently hold any professional certifications in the field of Cloud Computing?

Yes	4
No	21

5.Please select which professional certifications in Cloud Computing you hold (tick all that is applicable)

Amazon Web Services (AWS)	2
Microsoft Certified: Azure	1
IBM Certified Technical Advocate	0
Cloud Security Alliance: Certificate of Cloud Security Knowledge (CCSK)	0
Other	2

Other responses:
Oracle
CHFI, ECSA, CEH, CSCU, CTIA, CISSP, CEI;

6.Are you aware of the 4 principles defined by the Association of Chief Police Officers (ACPO) for digital forensic evidence processing?

Aware and use	3
Aware but don't use	9
Vague awareness and sometimes use	0

Vague awareness but not used	4
Not aware at all	9

7.Do you believe the current ACPO guidelines are sufficient for processing digital evidence within the Cloud?

Yes they are sufficient	4
No they are insufficient	6
Unsure	6

8.On a scale of 1-10 (**1 being least challenging - 10 most challenging**) how challenging do you feel a Cloud environments ability in collecting logs to aid a forensic or audit investigation

5.4 Average Number

9. On a scale of 1-10 (**1 being least challenging - 10 most challenging**) how challenging do you feel about the Clouds ability (from a system admins perspective) to access and provide relevant data to aid a forensic or audit investigation?

6.0 Average Number

10. On a scale of 1-10 **(1 being least challenging - 10 most challenging)** how do you feel relying on the Cloud Service Provider to aid forensics processes by providing the identification, preservation and ability to collect any evidence?

6.4 Average Number

11. On a scale of 1-10 **(1 being least challenging - 10 most challenging)** how challenging do you feel the integrity of the chain of custody is preserved within Cloud environments?

6.76 Average Number

12. On a scale of 1-10 **(1 being least challenging - 10 most challenging)** how do you feel multi jurisdictional issues (across various geographical locations) challenges Cloud environment forensics?

7.48 Average Number

13. On a scale of 1-10 **(1 being least challenging - 10 most challenging)** how challenging do you feel that evidence gathering from cloud environments can ensure integrity without contamination of data?

6.8 Average Number

14. *Optional* - Please provide any further challenges you believe Cloud Computing introduces to Digital Forensic processes

5 Responses:

1. One of the core selling points for cloud computing providers is their assertion that they have no access to the content of your data. Although they do log access, previous cases involving the likes of Apple/Amazon/Google/Facebook have demonstrated how reluctant the corporation's are to provide access to such data, beyond purely sovereign jurisdiction over where data is stored.

2. Distribution, data profiles can be reused to enforce consistency which contributes to efficient collection and analysis. International or regional/ state based law and GDPR are biggest obstacle.

3. Cloud computing is complicated because of the multitenant nature of systems, but it all comes down to a physical server,
the problems are not that it is a server (I can find out who owns the server and where it is located and use standard practices to process data, the issue is instead in the time taken to process a claim for the data (effective litigation hold) and trust in institutions to comply with requests.

4. NA

5. Cloud computing is complicated because of the multitenant nature of systems, but it all comes down to a physical server,
the problems are not that it is a server (I can find out who owns the server and where it is located and use standard practices to process data, the issue is instead in the time taken to process a claim for the data (effective litigation hold) and trust in institutions to comply with requests.

15. Please rank in order, **1 (top) being the highest impact**, the following categories that introduces the biggest challenge for cloud forensic functionality that would need most attention:

Rank	Options
1	Legal challenges - e.g. lack of legislation and multi jurisdictional issues
2	Technical challenges - e.g. various media formats, encryption, log gathering
3	Resource challenges - e.g. volume of data, time taken for analysis, training

16. At this point of the questionnaire, have you changed your mind on whether current ACPO guidelines are sufficient for processing digital evidence within the Cloud?

Yes I have now changed my mind	1
No, my opinion remains the same	15
I haven't heard of ACPO	9

17. Are you aware of a standardized framework for Cloud Computing forensic practices?

Yes	1
No	24

18.
Please specify the framework you are referring to

1
Responses
MI5

19. Please review the below proposed principle by Horsman (2020).

"All extracted and interpreted data deemed to be 'digital evidence' must have undergone robust testing and validation using accepted testing methods and peer review in order to verify accuracy"

Do you feel this is necessary to be mandated for inclusion in a standardized guideline framework for processing digital forensic data?

Yes	18
No	2
Useful, but not wholly necessary	5

20. Please rank **(1 highest - 9 lowest)** from the below list whether these pose challenges in the future for Digital Forensic processes.

Rank	Options
1	Encryption
2	Anti-forensic techniques
3	Complexity of Data
4	Legislation
5	Cloud Computing
6	Volume of Data
7	Privacy technology
8	Internet of Things (IoT) devices
9	Digital Forensic tool capability

21.Does the institution associated with you raise awareness of cyber security issues?

Yes	22
No	3

22.Do you feel more awareness/training is required to mitigate the threat from cyber attackers?

Yes	19
No	6

23.Do you feel your institution has processes in place and is prepared to respond to cyber security events particularly within the cloud environment?

Yes	17
No	6
Not applicable to my institution	1
Prefer not to answer	1

APPENDIX IV – INTERVIEW DATA SET

Full transcript from interview 1 and samples from interviewee 2 & 3

Interviewer: Hello good morning thank you for taking the time in participating to my research today.

Interviewee 1: Good morning, no problem at all.

Interviewer: I'd like to start off with a bit of your professional background and experience?

Interviewee 1: Certainly, I currently work in the information security department and my main role is to ensure my organisation is safe from threats to the security of sensitive information we hold within the organisation. This involves maintaining procedures, ensuring compliance and responding to incidents that occur within the organisation.

Interviewer: Thanks for that, can you advise if you hold any professional qualifications in relation to your role?

Interviewee 1: Yes I hold the AWS fundamentals certificate as well as internal qualifications within the company

Interviewer: And have you come across or heard of the Association of Chief Police Officers (ACPO) principles?

Interviewee 1: I have come across these yeah but do not directly apply to my role.

Interviewer: Can you maybe provide your views on how Cloud computing has on the impact on digital forensics or security in general.

Interviewee 1: There is certainly a fashion or trend at the moment to in not only computing solutions to the cloud but the vast expansion on Internet of Things (IoT) devices. Cost, efficiency and scalability seems to be the driving factor as well as passing on some responsibility of security and maintenance to cloud providers. I feel this is a great benefit as it eases the burden on the organisation itself and looks to expertise in the field who have a reputation and track record of delivering the required solutions. It has in turn, increased the reliance and potential complexity in supporting these systems but I feel as business demand grows as well as regulatory requirements force our organisation anyway to react accordingly and if that means adding complexity out of necessity then it has to be done. From a security perspective, having a reputable cloud solution from a reputable company transfers the risk and accountability to an extent but adds the risk of transparency of having third parties involved. It is therefore critical to establish regular lines of communications to ensure all service agreements are in check. All of these significant changes have in turn should warrant at least some sort of refresh of the ACPO to keep it up to date.

Interviewer: Going back to ACPO, do you feel given the changes cloud computing offers, do you feel ACPO practices maintain the integrity of evidence collected if and when required?

Interviewee 1: I think the cloud definitely adds challenges in the preservation and integrity of data from a traditional point of view. Not everything is stored locally on a hard drive for example and I am not sure if ACPO guidelines ensure the preservation of the A-Z of an evidence trail.

Interviewer: Is it safe to say then you feel gaps exist within ACPO principles in relation to be applied successfully in the cloud environment?

Interviewee 1: I would say so yes.

Interviewer: What I am going to do now is to read out 8 new principles that hypothetically replace ACPO and I would like your feedback on the suitability of these principles - if you feel I need to repeat these just let me know.

Interviewee 1: Sounds good

Interviewer: OK so the first principle is as follows:

Principle 1: “Any course of investigatory action undertaken by the practitioner must first be agreed upon by an appropriate authority, who themselves must have full knowledge and insight into any agreed course of action and the possible associated outcomes of such acts. Responsibility for the investigations course of conduct should be considered shared between the governing authority and the investigating practitioner.”

The newly proposed ‘Principle 1’ builds upon what was previously noted by ACPO as Principle 4; the principle of overarching responsibility. Whilst ACPO’s Principle 4 places responsibility on the overarching authority overseeing an investigation, it is proposed that responsibility should be viewed as a shared concept, between the investigating practitioner and the authority which governs/sanctions an investigation in the first instance. This is due to the fundamental differences in the roles (addressed below). There are three points of note to this principle:

1 All parties subject to the investigation must have full knowledge and insight into any agreed course of action, and foresight of the possible associated outcomes, before responsibility for investigatory decision making can be assumed. Whilst it is appreciated that investigatory unknowns may occur, this principle helps to prevent the blind commencement of processes which may subsequently turn out to be detrimental.

2 The governing authority is responsible for investigatory decision making at the law-enforcement procedural, policy making and investigatory levels. It is recognised that a governing authority may not also be a technical specialist and therefore the imposition of responsibility for technical decision making is unwise. Instead, responsibility for the imposition of investigatory powers and governance of investigatory conduct falls within their remit. This however does not preclude their decisions from being informed by their technical specialists.

3 The investigating practitioner assumes responsibility for their course of conduct and must assure adherence to the defined and agreed scope of an investigation, and to engage and uphold best practices and engage with quality assurance processes. In essence, the practitioner is responsible for the standard of their work and technical decisions, given their assumed expertise and knowledge of the processes involved with a digital examination.

Interviewee 1: That’s a long principle! But yes, sounds like common sense and builds on a previous ACPO principle I think you mentioned 4? Sounds like this just ensures the investigator is prepared and has the right knowledge and expertise in place which makes it a suitable candidate yeah.

Interviewer: OK and principle 2 now:

Principle 2:- “A practitioner and governing authority must understand those laws, policies and principles applicable to their given inquiry which define the scope of their investigatory powers. The practitioner must evidence adherence to these, and operate within their confines at all times”.

The newly proposed ‘Principle 2’ requires explicit knowledge of, and adherence to, those regulations and laws which define the scope of which a practitioner can exercise their powers of investigation. This does not necessarily place an obligation on the practitioner to understand the legal landscape of the offence in which they are investigating (although in most cases this will be beneficial to their investigation), but the legal powers governing their actions. It is their explicit duty to ensure they operate within these boundaries at all times, where conduct which strays beyond these confines creates practitioner liability for misconduct. This principle prevents a practitioner from straying into areas of questionable practice, claiming that they were unaware of any repercussions of their actions. This obligation is now more pertinent as more investigations are involving enquiry into non-local, cloud forms of storage where governance at presence may not be well defined and understood.

Interviewee 1: OK this sounds a little tricky and I'm wondering if this assumes knowledge of laws and polices across different regions. I think while useful and beneficial it is unrealistic and I don't feel it should be mandated within a standard framework.

Interviewer: Principle 3 reads as follows:

Principle 3:- "A practitioner should make all reasonable efforts to identify any and all sources of potential evidence relevant to their investigation, taking into account the concepts of proportionality and necessity in regards to any device/data which is seized/interrogated. All justifiable measures must be taken to limit both collateral intrusion and disruption caused by their investigation."

The newly proposed 'Principle 3' takes into account current policy and legal issues concerning privacy. It is acknowledged that the digital devices are embedded into the lives of many and their content can be of a nature which may cause distress to an individual should it be removed from their remit. There is also acknowledgment for the disruption which can be caused to the lives of individuals who utilise digital devices/data as part of their day-to-day functions and livelihood. Where feasible, practitioners should seek to only acquire data/devices which are pertinent to an investigation and in such cases (and where it is both possible and sensible to do so), provide for the prompt return of this content, ensuring disruption is kept to a minimum. This is particularly important given the current climate of digital forensics where backlogs and examination time delays are considered an unfortunate norm.

Interviewee 1: It sounds like a suitable proposition but I find it a rather long winded principle that can be ambiguous. But the guidance of ensuring where possible the identification of all sources of potential relevant evidence is important.

Interviewer: Principle 4 reads as follows:

Principle 4:- "A practitioner should only access digital data targeted by their investigation using a suitable method which is also compliant with Principles 1-3 noted above. A suitable method is one of the following:-

1 A known and accepted method, which has been subject to both peer and field-wide review, and appropriate testing and validation by the investigating practitioner who wants to use this method, and is lawful.

2 A developed novel method providing suitable testing and validation has been undertaken in order to verify its functionality, and is lawful.

In either case, the practitioner must understand the role of any method used and be able to explain its function."

The newly proposed 'Principle 4' draws reference to recent changes in the digital forensic landscape, where method validation and verification is now considered a core part of principles of quality assurance for digital examinations (see discussions regarding ISO17025 in the United Kingdom). Any examination of a digital device/data begins with access and subsequent acquisition of digital content. This process is fundamental and forms the foundation for any resulting investigatory work, meaning that methods used for carrying out these tasks must be reliable. Practitioners will often find themselves in one of two scenarios; the use of a known method or the use of a novel methods. A known method is only deemed suitable if it has been subject to both peer and field-wide review, and appropriate testing and validation by the investigating practitioner. Reliance on a method because it is the 'commonly done thing', is not enough to justify its use. Validation of the method by the investigating practitioner is required. The use of a novel method arguably carried greater risk, but the challenge remains the same. To be suitable, testing and validation must be undertaken in order to verify method functionality, and any findings must be documented and capable of scrutiny from peers. Now, schemes such as the Computer Forensics Tool Testing Program (CFTT) [18] provide transparent testing of tools, including those used for data acquisition and the Computer Forensic Reference Data Sets (CFReDS) offer a series of test data sets [19].

The importance of this principle cannot be understated, as with the level of difficulty placed upon adhering to it. Questions will be raised regarding the burdensome requirements proposed here, and the chances to adhering to this in real-world situations. However, the proposed principle provides a baseline level for quality assurance, where eroding the rigour of this requirement simply undermines the overarching purpose of having such principles, and inadvertently accepts substandard practices. The problem lies not with the proposed need for the field to ensure only suitable methods are used, but the pressures placed upon those working within it which prevent methods from being determined as suitable for use.

Interviewee 1: I think given the complications introduced by cloud computing, I feel it would be worthy of having methods accepted and peer reviewed to maximise admissibility in court and less susceptible to criticism. It sounds like a practice that ensures credibility and therefore suitable for inclusion.

Interviewer: Principle 5 reads as follows:

Principle 5:- "A practitioner should take all reasonable steps to preserve the integrity of any data/device(s) subject to investigation during the course of their examination."

The newly proposed 'Principle 5' is designed to preserve data integrity as far as is practicable, within the bounds of an investigation, providing acknowledgement to both the development of more advanced data acquisition techniques and the range of new technologies requiring more invasive methods in order to gain access to their data. This obligation is not absolute, as there are now many investigatory processes which require the manipulation of a subset of resident content in order to secure access to a great amount of data which a device/service may contain (seen with physical memory capture processes and some mobile device extraction techniques).

Interviewee 1: I am not sure how integrity is preserved on data that is outside your control or jurisdiction. With cloud computing I feel there are black box areas and things outside your control which potentially hinders ticking this box and hence not needed.

Interviewer: Principle 6 reads as follows:

Principle 6:- "Methods of access which compromise the initial state of digital data on a device must be utilised as a last resort. Where such methods are implemented, a practitioner must be competent to use these methods and the implications of their use must be both understood and capable of explanation by the practitioner. All efforts to capture and/or document any digital data prior to being compromised as part of these methods should be taken."

The newly proposed 'Principle 6' expands upon ACPO's Principle 2. Where a method must be implemented which may or is likely to compromise any existing digital data subject to investigation, the practitioner must fulfill three criteria:-

1 Be competent to use the method.

2 Understand the implication of using the method.

3 Be capable of explaining the method.

The requirement of competency must remain, preventing practitioners from blindly implementing procedures which they do not first understand. In addition, where a method may compromise a subset of data, the practitioner should first explore all possible options for capturing and recording this subset before it is compromised to allow greater data access.

Interviewee 1: This is important to ensure the practitioners is competent and understands the uses of these methods properly. The fact that this is an extension to ACPO principle 2 helps and should seamlessly be easy to include in an updated framework.

Interviewer: Principle 7 reads as follows:

Principle 7:- “All extracted and interpreted data deemed to be ‘digital evidence’ must have undergone robust testing and validation using accepted testing methods and peer review in order to verify accuracy.”

The newly proposed ‘Principle 7’ expands into territory previously uncharted by ACPO, and enforces an arguably important aspect for all investigations. ACPO make no comment regarding the need to test and validate findings, yet now in a time where forensic science is facing significant scrutiny over its quality management and assurance processes (and rightly so), it would only seem appropriate to acknowledge such a need. There has been much commentary regarding the potential mixed abilities and standards of work undertaken within the digital forensics field, where the imposition of effective testing is a method which in practice should reduce the chance of any misinterpretation.

Principle 7 is distinguished from proposed Principle 4 as this principle is directed at the practitioners interpretation of results.

Interviewee 1: Again I am unsure how cloud data can be 100% tested and validated for accuracy, I feel logs are the best source of evidence and maybe that can be tested to ensure no contamination has been applied but sounds like a very complicated task to be applied on a regular basis. I wouldn't include this in a newly proposed framework.

Interviewer: And finally, Principle 8 reads as follows:

Principle 8:- “All stages of a practitioners investigation must be documented, forming an audit trail which can be used to describe those processes implemented by the practitioner to a third party, and where necessary and possible, allowing these procedures to be repeated in order to obtain comparable results.”

The newly proposed ‘Principle 8’ acknowledges and expands upon ACPO’s Principle 3; the requirement for an audit trail. However, it is necessary to stress the use of the word ‘comparable’ in relation to describing results. In doing so, acknowledgment of the fact that some processes cannot be repeated is made, and that some processes can be re-run, but the results may not be the same (for example, RAM capture).

Interviewee 1: This should definitely be included, all stages of the evidence collection process should be audited and re-producible based on this record. It is in line with current ACPO guidance so this continues this type of behaviour.

Interviewer: Thank you for your inputs today, I’d like to finally ask you based on these proposed principles I note that you are in favour of most of them – can you maybe opine on whether you think these proposals should be a contender to update current ACPO principles?

Interviewee 1: Most of them did make sense generally but I also found them a bit more complex to follow than the current ACPO principles. I would say they need refining to make them more succinct otherwise you run the risk of these being mis-interpreted or even omitted due to regulation fatigue. While all these proposed principles are suitable in nature and certainly beneficial, in the real world to consistently achieve all 8 is not only complicated but unsustainable in an ever-growing dataset across wide ranging devices can place huge burden on those performing the work. I’d say a refresh is needed for sure, just a bit more succinct and easier to follow.

Interviewer: That’s all I have today this is really helpful and appreciate your inputs

Interviewee 1: No worries at all, those questions were fairly brutal by the way I feel I may have come better prepared seeing these in advance!

Interviewer: I actually have a questionnaire designed of which this interview is based on, maybe if you filled that in it would have given you a better heads up?

Interviewee 1: Yes that would definitely have helped.

Interviewer: Thanks again for your time and valuable feedback, have a good day!

Interviewer: You have commented on complexity on some of these proposals but you are still in favour for inclusion for these, can you maybe explain why you feel these should be included despite their complexity?

Interviewee 3:

Similar to the way technology advances and in turn cyber criminals look for ways to exploit – ACPO must at least reflect and mitigate any gaps created by advances to ensure the integrity and inclusion of digital evidence in today’s world.