Digital Forensic Analysis For Mac OS X

(1) SHILU DOLLYBEN NARENDRABHAI
P.G. Student in M.Tech.(Cyber Security) of Raksha Shakti University –Ahmedabad
(2) Mr.CHANDRESH PAREKH
Assistant Professor, Department of IT & Telecommunication
Raksha Shakti University – Ahmedabad

ABSTRACT

Digital forensic science is very much still in its infancy, but is becoming increasingly invaluable to investigators. A popular area for research is seeking a standard methodology to make the digital forensic process accurate, robust, and efficient. The first digital forensic process model proposed contains four steps: Acquisition, Identification, Evaluation and Admission. Since then, numerous process models have been proposed to explain the steps of identifying, acquiring, analyzing, storage, and reporting on the evidence obtained from various digital devices. In recent years, an increasing number of more sophisticated process models have been proposed. These models attempt to speed up the entire investigative process or solve various of problems commonly encountered in the forensic investigation. In the last decade, cloud computing has emerged as a disruptive technological concept, and most leading enterprises such as IBM, Amazon, Google, and Microsoft have set up their own cloud-based services. In the field of digital forensic investigation, moving to a cloud-based evidence processing model would be extremely beneficial and preliminary attempts have been made in its implementation. Moving towards a Digital Forensics as a Service model would not only expedite the investigative process, but can also result in significant cost savings – freeing up digital forensic experts and law enforcement personnel to progress their caseload. This paper aims to evaluate the applicability of existing digital forensic process models and analyses how each of these might apply to a cloudburst evidence processing paradigm.

Keywords: Digital Forensics as a Service, Digital Forensics, Mac OSX, Cloud Computing., digital forensic science.

1. Introduction

The field of digital forensics has become commonplace due to the increasing prevalence of technology sincethe late 20th century, and the inevitable relevance of this technology in the conducting of criminal activity. Intraditional forensics, the proof is usually one thing tangible that might establish the criminal, like hair, blood or fingerprints. In distinction, digital forensics deals with files and information in digital kind extracted from digital devices. Digital forensics could be a widely-used term, concerning the identification, acquisition and analysis of digital proof originating from way more than simply computers, like smartphones, tablets, net of Things Devices, or information keep within the cloud.

In the not-so-distant past, most cases involving digital rhetorical investigation concerned criminals exploitation computers, networks or alternative IT infrastructure as a tool for conducting their crimes. At that point, the set of devices requiring analysis sometimes consisted of one pc and also the cases involving digital investigation were sporadic. Society has become progressively dependent on a spread of digital devices, as a result, there's a massively redoubled would like for professional digital rhetorical analysis across a spread of cases, and a mess of devices requiring analysis per case has become commonplace. The increasing range of cases involving digital investigation; the quantity of digital devices requiring analysis is additionally increasing; the storage volume of every device is growing; the range of digital devices and also the numerous variety of storage formats, file systems, e.g., Internet-of-Things devices, wearables, cloud storage, etc., introduces further complexness to the digital rhetorical method. of these factors ultimately cause the mounting digital rhetorical backlog usually encountered in enforcement (Lillis et al. 2016).

integrate new technologies and methods over the previous model. The research on process models in recentyears, is more concerned with employing new methods and tools into the existing models to improve theefficiency of processing or dealing with the new problem in investigation

1.1 Digital Forensics as a Service

Cloud computing has become commonplace in today's world. As one example, cloud storage, such as GoogleDrive, Dropbox, Apple's iCloud, etc., are widely used by consumers around the world. The development ofcloud technology is a double-edged sword from a digital forensic perspective; the wide use of cloudinfrastructure and applications brings complexity to conducting digital forensic invesitigations, while leveragingthis on-demand, high-speed technology could also make much of the investigative process significantly moreefficient. However, based on the current literature in the area, 'Cloud Forensics' is much more popular, i.e.,recovering evidence from cloud services and applications. Research on DFaaS is still quite limited in the digitalforensic community.

DFaaS is very much still in its infancy. In the last decade, many corporations have finished their processing anddata migration from their own servers to the cloud service vendors, such as Amazon or Rackspace. Likewise, inthe process of digital forensic investigation, DFaaS could bring several improvements over the existing process.

1.2 About Mac OS X

For years, the Windows OS has been the mainstay ofenterprise computing, a common fixture in an ever-changingtechnology landscape. Though Windows continues todominate the enterprise market, Apple is taking bigger bitesout of its market share as the OS X ecosystem becomes anincreasingly popular business choice [9]. The business craving for raincoat devices is growing. Between 2011 and 2014, Apple sold-out over 3 million industrial units within the North American country alone. It's currently thought that Apple's share of desktop computers is around terrorist organization and growing by the day [10]. In fact, analysis suggests that ninety-six of companies currently support Macs within the work The increasing quality of Apple Macintosh hardware, notably that victimization Intel x86-compatible processors, provides new challenges and knowledge gathering opportunities for rhetorical examiners [8]. the times of associate OS avoiding attacks just by not being Windows is long behind North American country. Attacks against raincoat OS X and operative system} have each inflated significantly in 2016 and cyber security may be a necessity across the board for all operating systems—not only for Windows—to avoids the implications of attack [11]. raincoat OSX clearly needed distinctive methodology to analyze apple's systems. There area unit only a few forensics tools and techniques associated with raincoat OSX area unit out there within the market. The aim and objective of the analysis paper is to spot the supply of knowledge to gather artifacts with the assorted tool and techniques which is able to undoubtedly facilitate the investigator to analyse the $64000-time case to raincoat OSX.

2. The Evolution of Digital Forensic Process Models

Several process models have been proposed to date. Current models can be categorised into three main types:

● The first type consists of general models that define the entire process of digital forensicinvestigation. These models were proposed from 2000 to 2010. Through that time, precisely whatshould be done and the order to do each step in a digital forensic investigation was still somewhatcontroversial.

● The second type focus on a particular step in the investigation process or a specific kind of

investigative case;

● The third type defined new problems and/or explored new methods or tools to address specificissues.

3.Digital Forensics (The next generation of digital investigation tools)

A forensic investigation can be initiatedfor a variety of reasons. The most high profileare usually with respect to criminal investigation,or civil litigation, but digital forensic techniquescan be of value in a wide variety of situations,including perhaps, simply re-tracking steps taken

when data has been lost. [2]Digital investigationsand crime regularly cross international andlanguage borders today. Companies like BasisTechnology's next-generation Odyssey DigitalForensics™ products dissolve linguisticboundaries enabling analysts to searchmultilingually as easily as in English. TheComputer Forensics Toolkit was created byeminent practitioners, with many yearsexperience in the industry. The items includedhave been tried and tested in the field countlesstimes, and are in everyday use. [3]Odyssey cuts through technicalcomplexities that digital investigatorsincreasingly encounter: How to capture datafrom computers that may not be brought into thelab? How to search through data in languagesthe investigator doesn't know? How to take fulladvantage of the array of available digitalforensics tools, each with its own proprietary fileformats?

a) Capture: the Media Exploitation Kitenables experts and non-experts alike tocapture data off hard disks, while alsodocumenting the integrity and source of thedata.

b) Analysis: Odyssey Digital ForensicsKeyword Searching System's smart searchcrosses language and file format "barriers."Analysts need not know all the languages ofthe data to perform searches that quicklybring significant files to the fore.

c) Portability – the Advanced Forensic Format(AFF) for storing captured data is open and

extensible to make that data available foranalysis by any tool the investigatorchooses.

4.LITERATURE REVIEW

Philip Craiger, Paul K. Burke [2] - research paper focusedmore on the available artifacts from the system and user data.But it is necessary to recover the user deleted logs and historyof the OSX Applications to analyze the potential artifacts.Rob Joyce, Judson Powers, and Frank Adelstein [1] – Numberof OSX Application forensic has been mentioned in paperlimits the some artifacts related to FaceTime deleted history,Private browsing history for the Safari.

In today's modern world mobile phones are omnipresent containing people's daily life. Thus, mobile phones havebecome a digital repository, which includes all the basic information about the user from their daily scheduled meetingsto personal information. As such, the ubiquitous presence of mobile phones has led the smart/mobile phones to bepresent in all the illegal activities from child pornography to terrorism (Rakočević,, Pavlović, & Ivanović, 2017). In 2013,a 24-year-old man was arrested by Racine police because child pornography was discovered on his mobile phone(Fox, 2013). This is just one example of child pornography, there are millions of people arrested and data wasrecovered using mobile phone forensics analysis. Similarly, in the recent Paris terrorist attacks, mobile phones playeda vital role and facilitated the terrorists to elude intelligence services. As an article in The New York Times reports: "thethree teams in Paris were comparatively disciplined. They used only new phones that they would then discard,including several activated minutes before the attacks, or phones seized from their victims" (Moody, 2016).

Klomklin and Lekcharoen (2016) talk about how lawenforcement agencies in each country are using mobilephones in order to obtain information against criminals.They also talk about how improperly managing andcollecting of evidence can impact the investigation. Thispaper studies the mobile phones forensic procedure andexisting behavioural performance of law enforcement agencyin Thailand. Authors divided the study into 3 main steps: 1)studying general mobile phone forensics processing andprocedures. 2) Qualitative research using Focus groupincluded 20 experts from law enforcement agencies. 3)Quantitative research using 200 questionnaires. At the end,they provided a new framework of mobile phone forensicsprocessing and procedures for Thai law enforcementagencies. Quick and Choo (2016) developed a frameworkfor data volume reduction which focuses on the registry,documents, spreadsheets, email, internet history,communications, logs, pictures, videos, and other relevantfile types. When this framework was applied to theAustralian Law Enforcement Agency, the data volume wasslightly reduced leaving only the main evidential files anddata.

4. Digital Forensics as a Service

Even though, cloud computing has become prevalent across many industries, there is limited literature on itsuse and advantages from a DFaaS perspective (Lee and Un 2012; van Baar et al. 2014; Wen et al. 2013). In thissection, the current research on DFaaS will be discussed.

The first utilisation is the computing power provided by distributed computing, which can better handle theincreasing magnitude of data. Lee & Un (2012) shows the efficiency of cloud system working on indexedsearch. Wen et al. (2013) outline an implementation of cloud based system to combat the magnitude of dataencountered by digital forensics by leveraging parallel computing. This work highlights the applicability ofcloud computing in digital forensics and the improvement that DFaaS could make.One use case of DFaaS is to offer indexed search as a service (Lee & Un 2012). Concerning the large volume ofdata needing to be analysed, distributed computing systems could do the same work in parallel. Such cloudserver can offer highly intensive computing process and large quantity of storage to deal with the slowprocessing on big data volume. In their paper, Lee and Un outline a case study that indexed search as a service

5.Recent Research on Digital Forensic Process Models

Some new and popular technologies result in new problems hindering digital forensics investigations. Cloudcomputing makes evidence collection more difficult; Internet-of-Things adds a variety of new device andstorage forms; more digital devices connected into the Internet result in an ever-increasing volume of data. Inrecent years, research on process models is more focused on integrating other technologies, such as datamining, to support the original models, or propose novel process models to solve the issues caused by thesenew technologies.

Some recent models, as outlined in Figure 1, include

- An integrated conceptual digital forensic framework for cloud computing (Martini & Choo 2012).

- Data reduction and data mining framework (Quick & Choo 2014).
- Internet of Things (IoT) Based Digital Forensic Model (Perumal et al. n.d.).

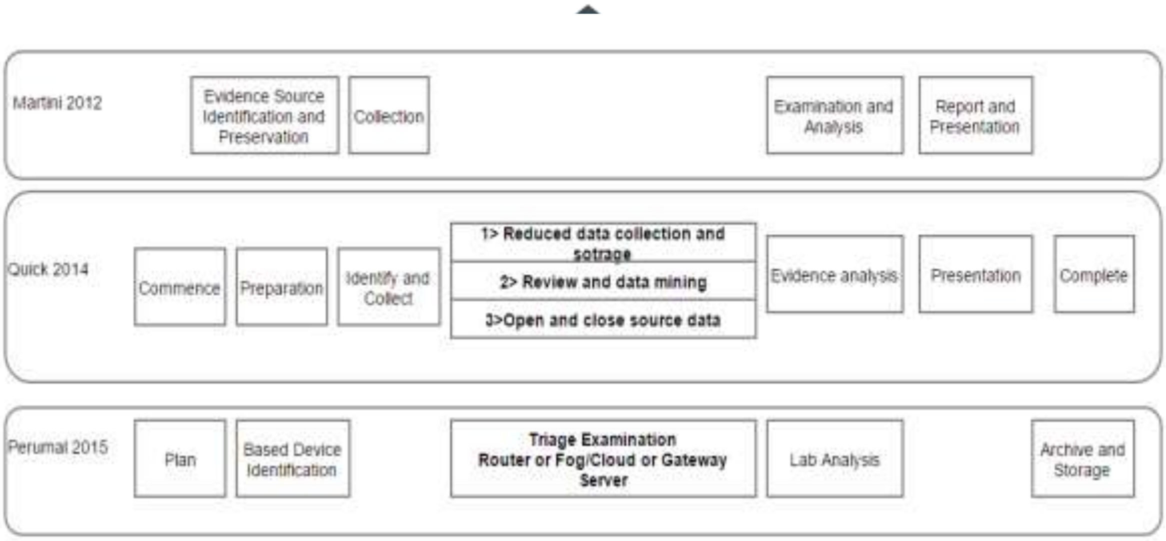
Martini 2012
Evidence Source Identification and Preservation
Collection
Examination and Analysis
Report and Presentation
Quick 2014
Commence
Preparation
Identify and Collect
1> Reduced data collection and sotrage
2> Review and data mining
3>Open and close source data
Evidence analysis
Presentation
Complete
Perumal 2015
Plan
Based Device Identification
Triage Examination Router or Fog/Cloud or Gateway Server
Lab Analysis
Archive and Storage

Figure (1) Recent Digital Forensic Models for Handling Modern Advancements

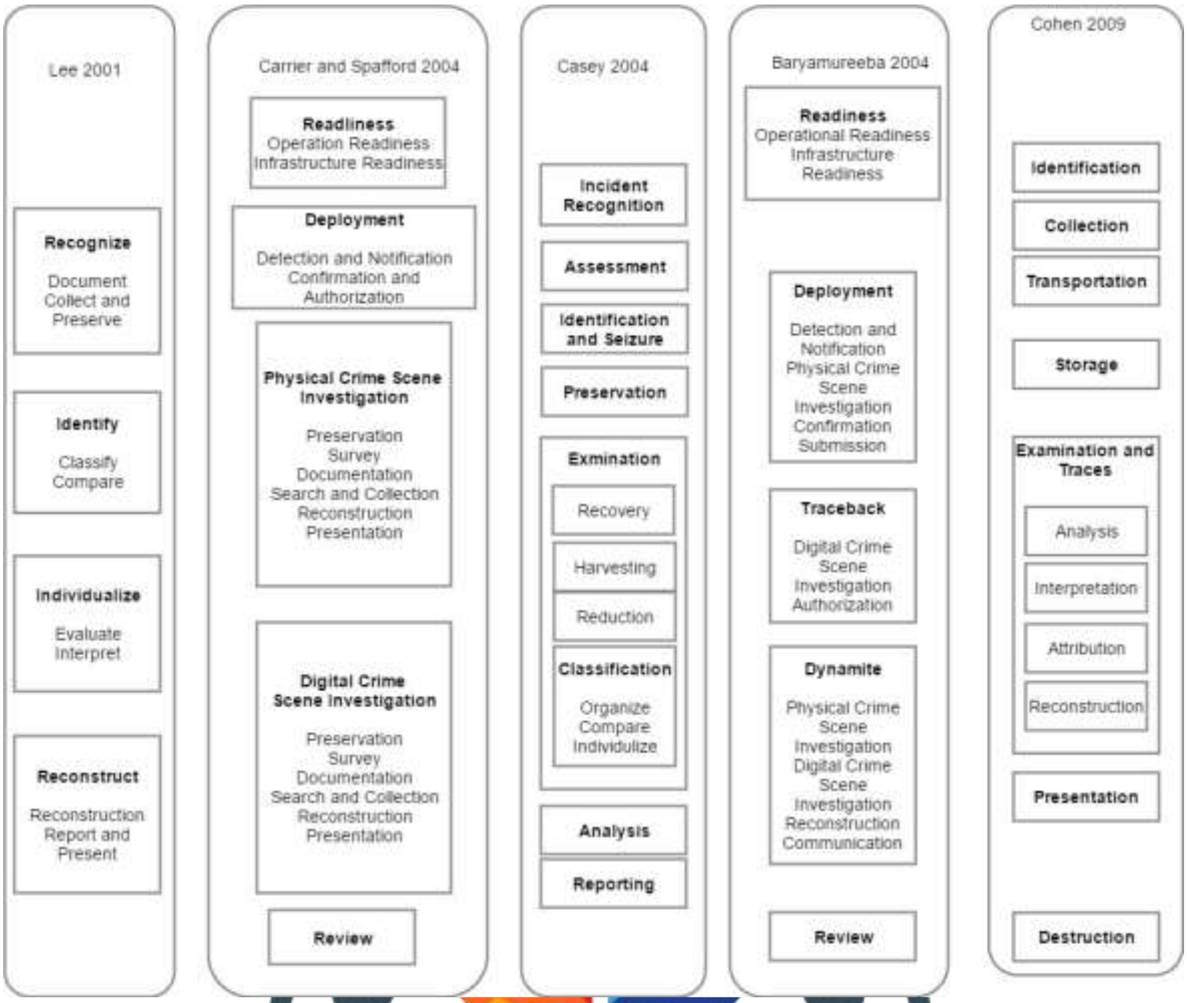

Figure 2: Digital Forensics Frameworks Focusing on a Specific Use Cases

6. Conclusion

A standardised procedure of investigation process is vital for conducting forensicinvestigations. The pursuit of a perfect model for digital forensic science will likely never cease. In this paper,the evolution of digital forensic process models was discussed and these models were classified into threetypes. The first type defines a general process for the entire investigation process. The second type refines andenhances the previous models by improving compatibility with more situations. The third type makes use ofnew methods, techniques and/or tools in the investigative process to deal with new problems encountered inmodern investigations. Overall, future refinements of the digital forensic process will likely focus on usagescenarios, improving the efficiency of the investigative process, and incorporating new technologies andtechniques into the models for the purposes of ensuring an always adaptable methodology.

5.1 Future Work

Society is increasingly moving their day-to-day life to the digital world. The huge volume of data has createdseveral challenges for digital forensics. By using theories and tools from data science to address these

challenges in digital forensics is a valuable research direction in digital forensics. Considering the significantinfluence which DFaaS could make in digital forensics, future work will focus on building an extensibleprocessing model focusing on the cloud-based handling of digital evidence.

RFERENCES

[1] Rob Joyce, Judson Powers, and Frank Adelstein. Mac Marshal: A Toolfor Mac OS X Operating System and Application Forensics. InProceedings of the 2008 Digital Forensic Research Workshop, 2008.URL: http://www. dfrws.org/2008/proceedings/p83-joyce_pres.pdf

[2] Philip Craiger, Paul K. Burke, "Mac Forensics : Mac OS X and theHFS+ File System," Department of Engineering TechnologyUniversity of Central Florida.

[3] Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C., 2011. Systematic Digital Forensic Investigation Model.

[5] International Journal of Computer Science and Security (IJCSS), 5(1), pp. 118–131.van Baar, R.B., van Beek, H.M.A. & van Eijk, E.J., 2014. Digital Forensics as a Service: A Game Changer. DigitalInvestigation, 11, pp. S54–S62.

[6] Baryamureeba, V. and Tushabe, F., 2004. The Enhanced Digital Investigation Process Model. In Proceedings ofthe Fourth Digital Forensic Research Workshop. pp. 1–9.

[7] Beebe, N.L. and Clark, J.G., 2005. A Hierarchical, Objectives-Based Framework for the Digital InvestigationsProcess. Digital Investigation, 2(2), pp. 147–167.

[8] Rob Joyce, Judson Powers, and Frank Adelstein. Mac Marshal: A Toolfor Mac OS X Operating System and Application Forensics. InProceedings of the 2008 Digital Forensic Research Workshop, 2008.URL: http://www. dfrws.org/2008/proceedings/p83-joyce_pres.pdf.

[9] State of Mac Security 2016 Enterprise Mac management, AvectoWhitepaper.

[10] Macs dent the enterprise, but not by much,By Esther SheinContributing Writer, Computerworld, MAR 24, 2016,http://www.computerworld.com/article/3047597/apple-mac/macs-dent-the-enterprise-but-not-by-much.html

[11] Internet Security Threat Report VOLUME 21, APRIL 2016 https://www.symantec.com/content/dam/symantec/docs/reports/istr-2 1-2016-en.pdf.