Digital Investigation 11 (2014) S54–S62

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Digital Forensics as a Service: A game changer

R.B. van Baar*, H.M.A. van Beek, E.J. van Eijk

Netherlands Forensics Institute, Laan van Ypenburg 6, 2497 GB The Hague, The Netherlands

Keywords:
Digital forensics
DFaaS
Digital forensic process
Process model
Xiraf

A B S T R A C T

How is it that digital investigators are always busy and still never have enough time to actually dig deep into digital evidence? In this paper we will explore the current implementation of the digital forensic process and analyze factors that impact the efficiency of this process. Next we explain how in the Netherlands a Digital Forensics as a Service implementation reduced case backlogs and freed up digital investigators to help detectives better understand the digital material.

Introduction

It is impossible to imagine life today without digital material. Who does not use a computer, smartphone, tablet or other digital device nowadays? As a result of the explosive growth in the number of devices and their use, the traces produced by the use of these devices have become more and more important in combating crime. This growth requires a new understanding of forensic data analysis: of the manner in which the data on these devices is processed and of the manner in which the traces collected by this processing is analyzed.

Since December 2010, in the Netherlands a new approach is used for processing and investigating the high volume of seized digital material, viz. Digital Forensics as a Service (DFaaS). Now, three years later, this approach has become a standard for hundreds of criminal cases and over a thousand detectives. This paper describes our approach and the impact on both the digital and tactical investigative process.

This paper starts with describing related work in the next section. In Section Traditional digital investigation process we describe the traditional digital investigation process, that we analyze in Section Analysis of the traditional process. The service model helps to solve a number of bottlenecks. The DFaaS model is described in Section Digital Forensics as a Service and analyzed in Section Analysis of the Digital Forensics as a Service Process. Despite the big changes this model causes, there is still room for improvement. In Section Experience and future work these improvements are discussed. Section Conclusions will complete this paper with final conclusions.

Related work

In this paper we apply a digital forensic process model to the previous and current digital forensic process in the Netherlands. In the related work we discuss process models, techniques that can help optimize the current process and expected developments that have an impact on the forensic process.

Process model

Even though the digital forensic process model is not standardized, consensus on the abstract level about the digital forensics process exists. The latest effort by Kohn et al. (2013) to propose a model contains an overview of the most significant models described over the years. On a high level, Kohn described six processes: *documentation*, *preparation*, *incident*, *incident response*, *digital forensic*

* Corresponding author.
E-mail addresses: ruud@holmes.nl (R.B. van Baar), harm@holmes.nl (H.M.A. van Beek), eijk@holmes.nl (E.J. van Eijk).

http://dx.doi.org/10.1016/j.diin.2014.03.007

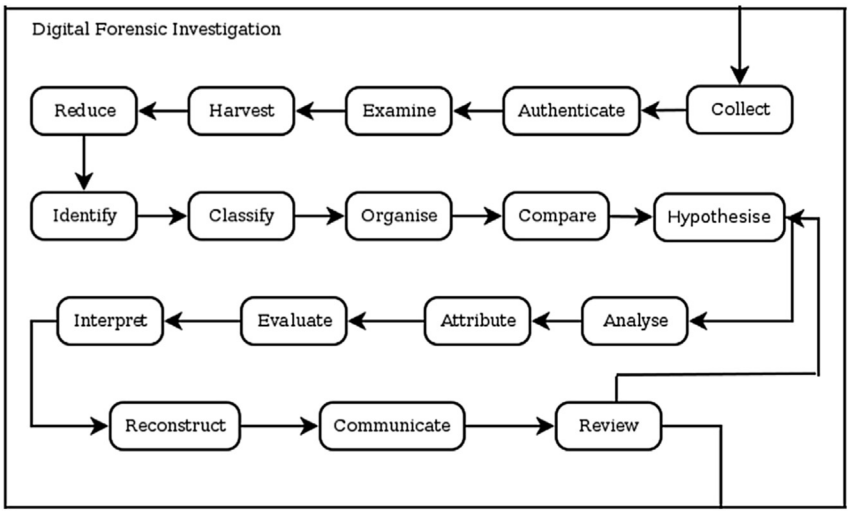

Fig. 1. IDFPM: Digital forensic investigation (Kohn et al., 2013).

investigation and *presentation*. In 2003, Carrier and Spafford already described the digital investigation process, where they defined five groups: *readiness*, *deployment*, *physical crime scene investigation*, *digital crime scene investigation* and *review*. Casey (2011) summarized the different steps as *preparation*, *survey/identification*, *preservation* and *examination/analysis*.

In addition to forensic investigations, eDiscovery exists. Their processes are very similar. Chisholm (2010) explains that the primary difference between the two is the scope of work. For eDiscovery, the Electronic Discovery Reference Model (EDRM)[1] is leading.

This paper focuses on the examination of the digital traces, defined by different authors as the *digital forensic investigation process* (Kohn), the *digital crime scene investigation* (Carrier) or *examination/analysis* (Casey). We explain how the digital forensics process is implemented in the Netherlands. We do this by using the integrated digital forensic process model (IDFPM) and terminology as described by Kohn et al. (2013), but other models can be applied just as easily. The *digital forensic investigation* step is presented in Fig. 1. Other parts of the IDFPM are described where applicable.

Technical implementations

Multiple next generation forensic analysis systems are under development or already implemented. These systems are generally built to automate and speed-up the indexing of the images, which is a good starting point to set up Digital Forensics as a Service (DFaaS).

In 2004, Roussev and Richard described a distributed processing system many times faster than AccessData FTK.[2] This was a lab setup. Since then FTK 3 and higher support a total of four so-called workers to automatically process data in parallel. Research on the automated processing of seized material was coined in 2006 by Alink et al. (2006). Ayers (2009) put down the need for such a system and described the requirements that such a system must, should or may meet. In 2012, Bhoedjang et al. explained how the Xiraf system is engineered and in use in the Netherlands. One of the efforts to build a DFaaS system is proposed by Lee and Un (2012). They focused on speed and provided the end-user with a web interface to search through the data.

A lot of tools exist that support eDiscovery in both law enforcement and businesses, like *ZyLAB eDiscovery OnDemand*[3] and *Symantec eDiscovery Platform*,[4] powered by Clearwell.

Expected developments

Some interest has already gone out to speculate on what will happen in the near future. Much of this speculation stays within the current boundaries and describes improvements in tooling and standardization. Richard and Roussev (2006) and Garfinkel (2010) described several developments they expected to happen. Some of these developments, like distributed processing, are already in production, as described before. Garfinkel expected a crisis in digital forensics if no efficient method is found to analyze all data. Some reasons for this are the increase in data, encryption and proliferation of operating systems and file formats.

Traditional digital investigation process

We discuss how the digital forensics process as described in Section Process model is implemented in the Netherlands. We do this by using the model and

[1] http://www.edrm.net/, visited Feb, 2014.
[2] http://www.accessdata.com/products/digital-forensics/ftk, visited Feb, 2014.
[3] http://www.zylab.com/services/ediscovery-ondemand- saas.aspx, visited Feb, 2014.
[4] http://www.symantec.com/ediscovery-platform/, visited Feb, 2014.