THE INTRICACIES OF ILLEGAL BYTES

Proving possession of and access to child pornography in the Netherlands

Y.M.M.J. van den Berg, LL.B.

Master's Thesis in Law & Technology

Under the supervision of dr.iur. S. van der Hof

and the examination of dr. C.M.K.C. Cuijpers, LL.M.

Tilburg University Law School, Tilburg Institute for Law, Technology & Society

TABLE OF CONTENTS

Acknowledgments

Thanks to H. Princen (*Politie Noord-Limburg, Digitale Expertise*) and E. van de Wiel (*Politie Midden en West Brabant, Digitale Expertise*) for their valuable time and kind assistance in taking me behind the scenes of digital evidence. Many thanks also to dr. Simone van der Hof. Her remarks were always invaluable and her optimism never failed to encourage me.

1 INTRODUCTION

1.1 Overview

The child pornography industry is one of the largest and fastest growing industries in the world. Various sources report that $20 billion is spent annually for online child pornography[1] and 20% to 30% of all pornography distributed online contains children. Although other sources claim these numbers are overblown,[2] none deny that the production and distribution of "visually recorded sexual abuse of children", as it is called, is a major problem to present-day society. For example, the Association of Sites Advocating Child Protection (ASACP[3])—an organisation that maintains a child pornography reporting hotline–reported in its most recent white paper[4] that 59% of the analysed images of child pornography feature children under the age of 11 and 31% even under 5.

The fact that the subject of child pornography can even be called an industry these days is to be attributed exclusively to the rise of the Internet. The American Department of Justice concluded in one of its reports[5] that child pornography was virtually non-existing in the mid-1980s: production and trafficking of such images was risky, difficult and expensive as a result of a series of successful law enforcement campaigns. The Internet changed all that. Suddenly there was global reach, a cheap and safe network for distribution and practically unstoppable means of spreading. As a result, the market for child pornography was reanimated, and investigators had to start all over again.

Production and possession of images depicting child pornography are criminalised in most countries, including both physical images (e.g. those printed on paper) and digital images (stored as a file on a computer's hard drive or other data storage device). For possession to be felonious, the images have to be held intentionally by the suspect. As it turns out, accidental possession of illegal files is not unlikely in the digital age. In the past decade several cases have sprung up, most prominently in the United States, in which the suspect claimed he[6] had no intent on possessing the images of child pornography that were found on his computer. Many different arguments have been brought up to support that claim: some quite far-fetched (the

---

[1] J. Brockman, 'Child Sex as Internet Fare, Through Eyes of a Victim', *New York Times* April 5, 2006, www.nytimes.com/2006/04/05/washington/05porn.html.
[2] See for an interesting discussion for instance www.radosh.net/archive/002308.html.
[3] www.asacp.org.
[4] Available at www.asacp.org/whitepaper/ASACP-whitepaper-9-10-2010.pdf.
[5] Available at www.justice.gov/criminal/ceos/childporn.html.
[6] Because sex offenders are mostly known to be men, this thesis will exclusively use male forms wherever gender marking is grammatically relevant. Note, however, that the number of female paedophiles is suspected to be severely underreported. See Cohen & Galynker 2009.

suspect's cat downloaded the images by walking across the computer keyboard;[7] the suspect was doing research for a book on Michael Jackson[8]), but others were more probable, particularly the following two often-heard accounts: firstly, the images of child abuse were—accidentally—included in a batch of adult pornography or other collection of files that the suspect downloaded, after which he tried to remove the illicit images (unsuccessfully, as it turns out); and secondly, a computer virus or other piece of malicious software must have downloaded or planted the child pornography without the suspect's knowledge. In short: nobody wanted those images or nobody knew how they got there, and it's up to digital forensic investigators to prove guilty beyond reasonable doubt.

In addition to the difficulties arising with proving intentional possession, the Lanzarote Convention[9] of 2007 introduced a new dimension to the criminalization of child pornography. Article 20 permits parties of the convention to criminalise the knowingly obtaining of access to child pornography, using information and communications technologies. This is an optional provision: section 4 of the article authorises member states to not apply, in part or in whole, the provision on accessing child pornography. So far, the Netherlands is the only country to have implemented it into its national legislation.[10]

1.2 Aim of research

In order to address the technical and legal issues that arise with proving intentional possession of and access to child pornography, the research for this thesis is based on and will try to answer the following question:

In what ways can digital forensic procedures successfully provide evidence in court to prove the intentional possession of, and the knowingly obtaining of access to child pornography?

The focus will be on the Dutch situation. The Netherlands is, at the time of writing, the only country in the world that has implemented the optional Lanzarote Convention

---

[7] D. Goodin, 'Man Blames Cat for Child Porn Downloads', *The Register* August 8, 2009, www.theregister.co.uk/2009/08/07/man_blames_cat/.

[8] 'Pervert caught downloading child porn claims he was 'doing research for a Michael Jackson novel'', *Northampton Chronicle* April 19, 2010, http://www.northamptonchron.co.uk/ (search for *child porn research*).

[9] Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (CETS 201). This convention came into force on July 1st, 2010, after having been ratified by five countries, including the Netherlands.

[10] Some American states have criminalised accessing. See for the case of Pennsylvania, for instance, www.mbm-law.net/articles/"viewing"-child-pornography-now-a-crime/656/. The Supreme Court in Oregon, in contrast, recently ruled that merely viewing child pornography online is *not* a crime: A. Green, 'Oregon Supreme Court rules that simply viewing child pornography on the Internet isn't illegal', *Oregon Live* January 6, 2011, www.oregonlive.com (search for *supreme court child pornography*).

provision on knowingly obtaining access to child pornography, and it is still unclear if and how both investigators and courts intend to apply this provision.

In order to break down both the research and the thesis, the abovementioned question is divided into several sub-questions. Each expatiates on a specific issue, and each issue will, by and large, be addressed in its own chapter.

The current state of affairs with regard to possession of child pornography will be the focus of **chapter 2**. What are the problems that arise with regard to proving possession of child pornography and with proving intent of that possession? What excuses have defendants come up with to deny intent of possession of illegal images found on their computer, and were any of those successful in court? What kind of technical means can computer users employ to hide the files on their hard drive and their activity on the Internet? The last part of the first chapter will include some educated speculation on the possible problems that are to be expected with regard to proving knowingly accessing of child pornography.

Chapter 3 will go into forensic procedures used to find suspects and produce digital evidence. What digital forensic procedures exist and which are of use to find suspects and evidence of their (intent of) possession of child pornography? How is this evidence treated and how is it prepared for use in court? How are those procedures regulated, both nationally and internationally?

Subsequently, **chapter 4** will follow the evidence trajectory into court. How are cases in which digital evidence is relevant in general, and those involving the possession or accessing of child pornography specifically, currently dealt with in court? How do judges regard the new phenomenon of digital evidence? Which types of forensic procedures do they accept and which, if any, do they reject and why?

Chapter 5 will present a critical reflection on the previous chapters and a look to the future of the legal battle against child pornography. Are there any efforts attempting to streamline the finding, securing and analysing of digital evidence, both nationally and internationally? What about high costs and other drawbacks of current forensic procedures, and how can they be improved in the long run? This last chapter will end with a conclusion of the thesis in which the research question is answered by aggregation of the answers to the sub-questions. Finally, some implications and limitations of the research will be touched upon.

1.3 Methodology

In order to find answers to all of the above questions, a combination of several research methods will need to be employed. This section will list and specify those methods.

First and foremost, an extensive literature review is required to provide an overview of the state of the art in academic research on the subject. This holds true for both the judicial side of the subject and the technical, forensic side. Although the subject of digital forensics can be considered something of a niche in legal doctrine, several authors have taken it upon themselves to compile extensive literature on the subject. Two authors in particular have, with the help of many others, written invaluable books on the subject: Stephen Mason and Eoghan Casey. The work of both authors will be referred to extensively throughout this thesis. Legal research in this field is predominantly published in (often American) periodicals and journals such as Digital Investigation and International Review of Law, Computers & Technology. Many articles have been written that have added something to the ever-growing field of legal digital evidence research, some of which are relevant to this thesis. This study includes elements of a comparative law research inasmuch as the information from the American periodicals will be projected back onto the situation in the Netherlands. The work of prominent Dutch criminal law scholars such as Corstens and Nijboer will be used to analyse the judicial implications of digital evidence in general and child pornography specifically.

Legal analysis will be applied to existing statutes and treaties, specifically the Lanzarote Convention and its implementation in the Netherlands. The drafts of that legislation can give insight into the choices made and the goals set by the particular legislative body and will help to determine if and how those goals have been met. A comprehensive study and analysis of past Dutch cases involving possession of child pornography should provide insight into how the courts regard the evidence of this offence.

Finally, two digital investigators have agreed to provide personal insight into the digital investigation process for the sake of this thesis. These interviews are conducted face to face in Breda and Venlo. A short questionnaire provides the basis for the conversation, but it is by no means restricted to written questions. The results of these extensive interviews will be interwoven throughout the text.

2 CURRENT STATE OF AFFAIRS

2.1 Possession of child pornography

The Cybercrime Convention[11] is an international treaty, aimed at harmonizing national laws with regard to computer and Internet crimes. At the time of writing, fifteen states have ratified the treaty, including the Netherlands. Article 9 of the Convention aims to criminalise, across the Member States, the possession of child pornography:

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*
   e. *possessing child pornography in a computer system or on a computer-data storage medium.*

This is reflected in the Dutch Criminal Code (DCC) in article 240b,[12] which reads, in part, as follows:

1. *He who distributes, offers, publicly displays, produces, imports, conveys in transit, exports, acquires, possesses, or accesses by means of a computer or communications service an image–or data carrier containing an image–of a sexual act involving or seemingly involving a person evidently below the age of eighteen will be punished with imprisonment of up to four years or a fine of the fifth category.*

A comparison between the Cybercrime Convention and the DCC sections reveals two disparities. Firstly, the required element of intent is nowhere to be found in the latter provision. Although intent is traditionally a written requirement in Dutch criminal law provisions, the legislator has acknowledged that, in this particular case, intent is implied to be an element of the offence. This has been confirmed in a Dutch Supreme Court case.[13] Secondly, the element of 'without right' has also not been adopted. The proceedings on the Cybercrime Convention don't mention it, but the explanatory report to the Lanzarote Convention, which contains a similar provision, provides some background into the clause: it allows Parties to provide for discretionary defences regarding uses of dubious images in the fields of art, science and the like. The Netherlands has not done so.

Consequently, there are three distinct elements to both provisions that might prove troublesome in practice: the question of which images constitute child pornography,

---

[11] Council of Europe Convention on Cybercrime (CETS 185).
[12] Translation by the author.
[13] HR 28 February 2006, *NJ* 2006, 179.

the element of possession thereof, and the fact that this possession has to be intentional. Although the first element is an interesting and important question in and of itself, it will not be covered in this thesis. The focus here will be on the elements of possession and intent.

2.1.1 Possession

Article 9 of the Cybercrime Convention specifically mentions possession of child pornography *in a computer system* or *on a computer-data storage medium*. The DCC provision is not limited to possession in computers, although it is expected that child pornography depicted in physical media, such as magazines, is virtually non-existing.

The wording of the provision in the Cybercrime Convention suggests that possession of child pornography on *someone else's* computer system is quite possible: it doesn't seem to require that the suspect stores his collection on his own computer or other storage medium. Having said that, investigation into possession and, more specifically, proving this possession, pose a number of problems that law enforcement has to cope with. This subsection provides an overview of those problems; how these are tackled by law enforcement is the focus of the next chapter.

The investigative process starts with locating illegal images. Investigators in most countries have coercive power to conduct a computer search, but—for good reason—not without a reasonable suspicion of criminal activity. Most computers these days are network-connected in some way, particularly to the Internet, which provides investigators with more ways to monitor activity, but for both practical and privacy reasons, constant monitoring is impossible. Fortunately, investigators can be assisted in this matter, for instance by subscription-based online services, which not only include Internet Service Providers, but such facilities as Usenet newsgroups and Yahoo!-Groups, through which images of child pornography are often exchanged; conglomerate organisations such as the Financial Coalition Against Child Pornography,[14] a collection of several financial institutions that monitor transactions which finance child pornography; and everyday IT technicians and computer repair services, often reporting to the police when they find something illicit.

The next step is following this digital trace to a physical computer and confirming that the images are indeed there, by conducting a search of the computer's hard drive. As stated above, computer searches are often provided for in criminal procedure statutes[15] (either specifically or through regular search and seizure provisions), but that doesn't mean investigators are sure to find anything: computer users can employ countless techniques for hiding files or otherwise obstructing access to them and,

---

[14] 'The Financial Coalition Against Child Pornography Fact Sheet', www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703.

[15] The parties to the Convention on Cybercrime are required to have such a provision, based on article 19 of the Convention.

although digital investigators do what they can to keep up with these techniques, it is quite possible that many files are successfully removed from view this way.

The easiest way of hiding a computer file is, of course, simply deleting the file. As it turns out, this often poses little problems to digital investigators, since deleted files, even those permanently erased by emptying the recycling bin, still linger in unused sectors of the hard drive and are easily retrieved. However, other techniques are harder to deal with. Computer users can employ encryption[16] for certain files or the entire computer to scramble the contents and without the password[17] required for unscrambling the information, it is unreadable or inaccessible. There are several software programs readily available that claim to hide files without leaving a trace. Other programs allow a user to easily alter the hash value of a file, which are often used by investigators to search for known illegal files. Remote storage is a method which allows a computer user to store files on another computer elsewhere, but access them—with the right password—from his home computer. Even more problematic is cloud-computing storage—a variant of remote storage that puts the user files on a remote server only known to the cloud service provider. Finally, kill switch devices are available that allow a computer user to instantly wipe a hard drive with the press of a button.

This is an overview of just some difficulties that investigators might encounter when searching for evidence. Although quite technical in nature and not known to the average computer user, some child pornographers are quite familiar with them. For instance, the 'Traders Security Handbook' was a guide that was shared between the many suspect in the huge Wonderland child pornography case in the UK. It contained extensive instructions on how to hide images and what to do when caught.[18]

The next matter arises when images have been found: there is now some form of possession, but not yet a suspect. Most often, the owner of the computer will be the logical suspect, but it may be difficult to pinpoint a possessor if multiple people regularly use that particular computer, for instance in a family home or office. In a Dutch case from 2009,[19] the suspect's computer was found to contain child pornography, but neither the digital investigators nor the judges could say with enough certainty that it was the suspect who put it there: his friends and mother used the computer ever so often, and hence the suspect was inescapably acquitted.

---

[16] High-end versions of the Microsoft Windows Vista and Windows 7 operating systems include BitLocker Drive Encryption, a feature that allows full disk encryption. Apple Mac OS X has included a similar feature called FileVault since version 10.3. Separate software packages such as TrueCrypt (www.truecrypt.org) are also available.

[17] Note that, in the Netherlands, investigators can order the decryption of data or the production of the encryption key, but this order cannot be directed at the suspect, due to his privilege against self-incrimination.

[18] Ferraro & Casey 2005, p. 194.

[19] Rb Zutphen 18 November 2009, LJN BK3748.

2.1.2 Intent

Once illegal images have been found and linked to a certain suspect, his intent on possessing those images has to be proven: there is always a chance the child-abusive material ended up in the suspect's possession by accident. Indeed, virtually every suspect denies intent and has an excuse ready for the presence of illegal material on his computer, some of which are certainly plausible, at least from a technical point of view. The following examples are American, since reports on those cases are readily available, but both the factual and legal ramifications of these cases are not at all restricted to the United States.

In 2009, Matthew White from Sacramento[20] intended to download a particular file of adult pornography through a file sharing computer program, but discovered—upon completion of the download—that the file contained child pornography. White immediately deleted the file but investigators recovered it and he was charged with possession of child pornography.

Another example is the 2006 case of Nathaniel Solon,[21] also a user of file sharing programs. The defence alleged that Solon's computer was infected with a particular virus that downloaded child pornography automatically. Investigators followed the illegal images to Solon's computer and arrested him for knowingly possessing images of child pornography. Solon is currently serving a 72-month prison sentence.

The most prominent example of a lengthy case in which a suspect *was* eventually cleared of charges is the case of Michael Fiola. Child pornography was found on his company laptop when Fiola's bosses investigated the computer's excessive data traffic within the company. He was subsequently charged, but decided to privately fund a defence investigation on the laptop. The independent forensic examiner he employed found multiple viruses and Trojans that allowed the laptop to be compromised. The computer was directed to visit over forty malicious websites per minute, often at times when Fiola did not even have access to the computer. The examiner concluded that not only couldn't Fiola have downloaded the material—he probably wasn't even aware that it was there. In the end, the charges against Fiola were dropped, but not after he had lost his job, friends and life savings.

Michael Fiola's case seems to confirm that it is possible for a virus or Trojan to take automated control over a computer system and direct it to downloading all sorts of unwanted files. In the similar 2004 case of Julie Amero, this statement was taken to court and indeed acknowledged by the judiciary, although it took the overturning of the original conviction and a new trial, years later, to reach that verdict. Amero, a substitute teacher, was charged and convicted for risk of injury to a child when the

---

[20] J. Van Grove, 'Man Downloads Child Porn "Accidentally," Faces Up to 20 Years in Prison', *Mashable* December 5, 2009, www.mashable.com/2009/12/05/child-porn-download/.
[21] Solon's story has been documented on the website www.framedforchildporn.com.

classroom computer started to show random (adult) pornographic website pop-ups to the entire seventh grade. The prosecution believed Amero to have visited these websites purposefully, and the jury agreed. She faced a prison sentence of up to 40 years. It once again took a private investigation, this time by a team of professional computer experts, to point out the evidence in favour of the suspect. They were able to do so solely based on the information presented at trial, which indicates the grave technical errors that were made by both the prosecution and the defence in assessing the evidence during the legal proceedings.

The trouble, of course, with accepting this defence is that every suspect is eventually going to use it. In 2004, Matthew Bandy, an Arizona 16-year-old, was charged with possession of child pornography after investigators followed a report on an exchange of child-abusive material through an Internet social group to his computer. Not only was illegal material found on his computer's hard drive, but also on a recordable CD that was kept by the suspect. Bandy claimed it must have been a virus, and the Bandy family hired an investigator—the same forensic investigator, in fact, that Michael Fiola hired for his defence, with equal success. She allegedly found a combination of several viruses and Trojans that instructed the computer to download child pornography. Matthew Bandy was eventually convicted for a frivolous minor offence.[22]

Opinions on these proceedings vary greatly. The district attorney points out in his memorandum[23] on the case that, for all the things computer viruses and Trojans are capable of doing, they cannot put an empty recordable CD in the CD drive of the computer, write files to this CD, eject it, label it, and put it on a shelf.

It is clear that sufficient technical expertise with law enforcement, prosecution and judiciary is crucial in cases such as these. Criminal intent can only be proven by relying on evidence found at the crime scene, and with computer crimes such as possession of child pornography, the suspect's computer embodies that crime scene.

2.2 Accessing child pornography

A recent development in the combat against child pornography has come up in 2007, when the Council of Europe drafted its Convention of the Protection of Children Against Sexual Exploitation and Sexual Abuse. It added to the existing Cybercrime Convention provision a new dimension to incrimination of end-users of child pornography. Article 20, section 1 of the Lanzarote Convention reads, in part, as follows:

---

[22] W. McElroy, 'In Child Porn Case, Technology Entraps the Innocent', *Fox News* January 16, 2007, www.foxnews.com/story/0,2933,244009,00.html.
[23] Available at drumsnwhistles.com/pdf/bandy-case-report-02-01-07-mirror.pdf.

Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:

f. knowingly obtaining access, through information and communication technologies, to child pornography.

The explanatory report on the Lanzarote Convention explains the provision in more detail: it is intended to criminalise the accessing of child pornography websites, without downloading the available images. Criminal liability exists on two conditions, according to the Council: the suspect must intend to visit a site where child pornography is available and he must know that child pornography can be found there. Both of these conditions ought to make sure accidental visiting of such websites is not penalised.

The Netherlands has incorporated this clause into the existing provision on criminalisation of child pornography, article 240b of the DCC, as follows:

1. *He who (…) accesses by means of a computer or communications service an image—or data carrier containing an image—of a sexual act involving or seemingly involving a person evidently below the age of eighteen will be punished (…).*

In the explanatory report to the bill for this update, the Dutch legislator specifically mentions it is not intended to criminalise the actual *viewing* of illegal material, because that would simply be impossible to enforce. The legislator and academic literature in the Netherlands consider this provision to cover a possible gap in the Dutch criminalisation of possession, in which the suspect accesses child pornography websites but does not download and save images, and is furthermore technically experienced enough to meticulously erase any and all traces of his activities from his computer's hard drive. Now, these cases can no longer—theoretically—escape litigation.

However, the fact that there is a legal framework for prosecution doesn't mean those accessing child pornography will be caught easily: the problem of proving intent remains. The Lanzarote Convention Explanatory Report provides two suggestions on how to go about this: intent on accessing is evident when the suspect accesses those sites recurrently, or when he is found to have paid for such access. The Dutch legislator adds to this some concrete indications for illegal accessing: when the suspect is found to have followed a hyperlink that clearly hints at illicit material, or when he possesses login credentials to child pornography websites.

The team High Tech Crime of Dutch law enforcement acknowledges the importance of the provision, but emphasises that this criminalisation is in no way a certainty that all access to child pornography in the Netherlands will be found and prosecuted.[24]

---

[24] *Kamerstukken II* 2008/09, 31 810, No. 3, p. 5.

The team mentions several key problems that make it hard to successfully investigate access to child pornography websites. Suspects can reroute their connection to hide their presence on the Internet. They do this by employing proxy servers: specific server computers that can be used as an intermediary for internet traffic requests, effectively hiding the presence of the suspect's computer behind it. Especially by employing several of these proxy servers in succession, each linking to the next, it will be very hard if not impossible to trace a connection.

Another problem, one common to all cybercrimes, is that of globalisation: if internet traffic crosses state borders—and in the case of child pornography, it practically always does—international police cooperation needs to be called upon which, despite all efforts, is still working cumbersomely.

3 FORENSIC PROCEDURE AND REGULATION[25]

3.1 Digital forensic science

3.1.1 Introduction

The easiest possible evidence for possession of child pornography that investigators can find is the presence of such material, in plain view, on the suspect's computer. Of course, it is rarely that simple, and those investigating the offence have employed more advanced methods of examining the suspect's computer in order to find traces of evidence to prove the suspect indeed possesses child pornography.

Practically every computer use leaves traces on that computer. For instance, the operating system of a computer records user logon times and duration of sessions. Creating a file records the creation time. Editing that file leaves a last-edited timestamp on that file and an entry in the "Recently Opened" list. Connecting the computer to a network such as the Internet leaves even more traces. Visited websites are thoroughly recorded in the browser history, and a duplicate of those sites is copied into the browser cache. Network logs on the computer keep details on connection times, and the Internet Service Provider (ISP) through which that computer is connected usually records the same information. Most file transfer systems keep logs that record each transfer of files. Ferraro and Casey put it best when they said that "in essence, every action on a computer, including creating, downloading, viewing, printing, encrypting, and deleting files, can leave traces on a disk and in the Registry."[26] The French Forensic scientist Locard wrote his famous 'exchange principle' in 1927, and it is still relevant in the digital world: when a person enters and leaves a crime scene, that person will inevitably exchange evidence with the scene.

Most computer users are unaware of these traces, but specifically trained investigators of law enforcement and other agencies can find and recover this digital evidence.

---

[25] The meat of this chapter is based on the work of Ferraro, Casey and Mason, and has been filtered and organised to fit the particular cases of possession of and access to child pornography.

[26] Ferraro & Casey 2005, p. 85.

3.1.2 Digital evidence

Computer files and traces of computer use can be used in court as evidence to support the conviction of a crime. The collective term used for this rather new form of evidence is 'digital evidence'. Mason defines it as follows:

"Data (…) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication"[27]

Dutch law specifically defines data as "any representation of facts, conceptions or instructions suitable for transfer, interpretation, or processing by persons or automatic appliances."[28]

Digital evidence is not just important to cybercrime cases, but can be relevant in investigations of all crimes and even civil cases: computers are an integral part of everyday life and, as such, are a considerable source of evidence. Mason goes as far as saying that digital evidence is now the major form of evidence.[29]

An important distinction to make here is that between class characteristics and individual characteristics of evidence.[30] All evidence has class characteristics.[31] Evidence that has class characteristics (also called 'class evidence') does not tie to a particular suspect but rather connects to a particular class. Consider the following example: type of printer, make of hard disk. The suspect must possess these. From this follows that obtaining a large amount of evidence with class characteristics is just as good as finding evidence with few individual characteristics: the more class characteristics are found, the more it narrows down the list of possible suspects that fit that evidence. Individual characteristics are more valuable, but harder to acquire, since not all evidence has them. Individual characteristics are unique and are produced on a (physical) object by use, abuse or corrosion. Individual characteristics on a file make that file unique and can connect it to a particular source with high degree of probability. Examples include recorded serial numbers, scratch on lens that leaves a mark on the images taken with that camera, etc.

3.1.3 Digital forensic science

The field that concerns itself with finding this digital evidence is called digital forensic science.[32] It is a broad field and covers more than just child pornography: computer

---

[27] Mason 2007, p. 22.
[28] Article 80quinquies DCC. Translation by Pijnen & Fennell-van Esch in: Mason 2008, p. 628.
[29] Mason 2008, p. xxxviii.
[30] Casey 2004, p. 97.
[31] 'Class and Individual Characteristics', www.nij.gov/training/firearms-training/module06/fir_m06_t04_05.htm.
[32] Different authors use different terminology regarding this field. 'Digital forensic science' is a term proposed by the Digital Forensic Research Workshop, and will be used in this thesis. It should be noted that 'forensic computer analysis', 'forensic computing', 'digital evidence

crimes such as hacking, phishing and child grooming are just a few examples of offences that are investigated primarily through digital forensic science. Furthermore, more traditional crimes warrant a digital investigation as well, when a computer has played a major part in the crime, for instance in facilitating communication between the individual offenders.

Casey defines forensic science as "the application of science to law". He particularly stresses the science part, in that investigators should use scientific methods in their investigation, specifically the scientific method of *falsification*. In reconstructing the crime based on the evidence, investigators should develop many theories and try to find flaws in all of them, rather than sticking to a single hunch. Although it is easy to fall prey to preconceived theories, even more so when the investigator is experienced and the crime at hand regards child pornography, which carries a rather emotional weight, investigators should at all time remain objective. Concentrating on a single theory more often than not results in investigators only finding evidence that supports that theory and ignoring or failing to find exculpatory evidence that refutes it. It is for the investigators to focus on facts; courts will decide on the truth.

3.1.4 Digital vs. physical evidence

Digital evidence differs from traditional, physical evidence primarily in that it is volatile, time sensitive and easily altered. In essence, digital evidence is nothing more than a series of ones and zeroes, arranged in a particular pattern and electronically or magnetically held on or in an electrically powered storage medium. Although it is true that computer data is easily altered (either intentionally or unintentionally), courts worldwide have accepted the use of digital evidence to support a conviction. With careful conservation and authentication, digital evidence can be just as reliable as more traditional evidence.

Additionally, digital evidence is subject to rapid technological changes and wholly intangible, adding up to such a degree of complexity that many legal minds have a hard time in comprehending the possibilities and intricacies of digital evidence, or simply avoid attempting such comprehension.

Finally, digital evidence is circumstantial,[33] in that it is left by computer activity, not human behaviour. Although both are intrinsically linked, it might prove hard for investigators to link this computer activity to a specific person.

3.1.5 Preservation of evidence

The notion of careful preservation should be significantly present throughout the investigative process. The adverse characteristics of digital evidence discussed

---

examination' and the like all represent the forensic science that analyses and examines digital evidence.

[33] Casey 2004, p. 17.

above are such that incorrect recovery, handling or storage of the evidence can alter or destroy it, obviously deteriorating its value in court. This concept of 'evidence dynamics', as it is called, can be avoided by making strict operating procedures for all investigators handling the evidence, which dictate the course of action for successfully handling and preserving digital evidence without altering it, ultimately to maintain evidential continuity and integrity of the evidence.[34]

An important element in this preservative process is keeping a chain of custody: an extensive documentation of the entire handling process of a particular piece of evidence. It contains information such as who collected the evidence, how and where it was collected, who took possession of it, how and where it was stored and under what protection, etc. Correctly recorded, it proves in court that the evidence is authentic and unaltered, should the defendant challenge this.[35] More practical measures towards preservation include putting tape around the computer case to stop investigators from haphazardly opening it, putting loose hard drives in antistatic bags to prevent damage to the drive from electrostatic discharge, and so on.

3.2 Evidence of possession of child pornography

3.2.1 Finding suspects

Child pornography is exchanged almost exclusively via the Internet. Contrary to popular belief, the term 'Internet' is not the name of the service to access websites: the Internet is only the 'network of networks' that facilitates this service. Websites are part of what is called the World Wide Web (the 'www' in most URLs), but this is just one of several features the Internet offers, next to e-mail, Internet telephony (Voice-over-IP, or VoIP), newsgroups, online chat and peer-to-peer networking. The World Wide Web has a rather slight role in the exchange of child pornography, since child pornographic websites are usually shut down as soon as they are discovered[36] or purposefully taken down because of fear of detection. As it turns out, the other Internet services are much better in fulfilling the goals of criminals in the exchange and acquisition of child pornography: they are not (or less) public and activity is more easily hidden. Even Bulletin Board Systems (BBS), a historical dial-up service to connect users, are now used to exchange child pornography underground, because they are separate from the Internet and therefore harder to trace.[37]

There are three general ways in which investigators can pick up a cyber-trail to direct them towards a possible crime of possession of child pornography: they can receive

---

[34] Mason 2007, p. 47.
[35] Mason 2007, p. 50.
[36] Wortley & Smallbone 2006, p. 9.
[37] Ferraro & Casey 2005, p. 33.

a report on the matter, they can actively seek out such crimes themselves, and they can come across child pornography while investigating other matters.

Reporting

Many investigations into possession of child pornography have had their origins in a report from a third party. ISPs usually have the technical means to monitor web traffic of their subscribers and some do, reporting any occurrence of illegal material directed towards an individual to the police. Online services such as forums and communities are generally moderated for illicit content. Financial institutions are in a proper position to report child pornography, since much of the material is not freely available and requires a commercial transaction. The Financial Coalition Against Child Pornography has been mentioned before as a gathering of several such institutions to collectively combat child pornography.

Parties that are closer to the suspect might be in an even better position to report. Computer repair shops are often the ones to report child pornography they find on a client's computer. Employers typically monitor computer and Internet usage and have been known to report suspicious behaviour of their employees. A recent case in The Hague[38] started with the system administrator of the suspect's office noticing curious Internet activity from the suspect's workstation and reporting this to the police.

It should be noted that there is a duty to report certain serious crimes in the Netherlands, but possession (or, for that matter, production) of child pornography is not among those offences,[39] although police do encourage this type of reporting by any party.[40] A service has been set up as early as 1995 to facilitate anonymous reporting of child pornography on the Internet.[41]

Actively seeking out

Most trade in child pornography takes place at what are called the "hidden levels of the Internet"[42]; a simple Google search would not suffice to find this trafficking. Usenet is an often-used means in the exchange of child pornography, and the use of this service can be carefully hidden and encrypted, and even prevented from being archived, as is commonly and automatically done with all Usenet postings. Internet Relay Chat (IRC) is also popular by child pornographers; IRC can equally be hidden very successfully and participants in the service are anonymous. There is no central server to IRC and it supports a feature called Direct Client Connection, which directly

---

[38] Rb The Hague 26 November 2010, LJN BO5163.
[39] 'Doen van aangifte ernstig misdrijf, verplichting', overheidsloket.overheid.nl/index.php ?p=product&product_id=11662. Such a duty to report does exist, for instance, in the United States, as stated in Section 13032(b)(1), Title 42, Chapter 132, Subchapter 4, US Code.
[40] 'Aangifte doen niet verplicht voor reparateur', *BN De Stem* June 18, 2009, www.bndestem.nl/ algemeen/binnenland/5131208/Aangifte-doen-niet-verplicht-voor-reparateur.ece.
[41] www.meldpunt-kinderporno.nl.
[42] Wortley & Smallbone 2006, p. 13.

connects two chatters and enables them to exchange files, leaving little or no evidence on the IRC server. IRC can even be encrypted. Peer-to-peer (P2P) networking, a third Internet service that allows the exchange of files, shares these characteristics of concealment if done properly.

All these features of these services make it practically impossible to trace any trafficking of child pornography. Considering that, the most successful way of unearthing criminal activity is an undercover operation, in which investigators participate in the trafficking, trying to offer child pornography to paedophiles, using Usenet, IRC, P2P or other similar services. Honeypot websites are put up by law enforcement specifically for this purpose. These are offering pornographic images in exchange for credit card details. When visitors of these sites steadfastly continue on to the child pornographic section of the website, after receiving several warnings thereof, their credit card information is recorded and they are subsequently sought out. Investigators can similarly infiltrate into a Usenet or IRC paedophile ring, trying to gain the trust and respect of its members by contributing some child pornography, and subsequently working out the IP address of those members in order to apprehend them.

However, undercover undertakings such as these are not without their problems and risks. Seasoned child pornographers have learned to be particularly cautious for police sting operations. Wortley & Smallbone argue that sting operations only catch inexperienced and low-level offenders, because the more significant offenders are technically experienced enough to avoid detection.[43]

Accidental stumbling on

The third category, mentioned briefly here, involves investigators fortuitously stumbling upon child pornographic images during the investigation of a separate and unrelated crime.

3.2.2 Sources of digital evidence

After picking up the cyber-trail and connecting it, via an IP address[44] or credit card information, to a physical address, investigators will want to search that physical location for the child pornography to confirm their suspicion.

Generally, any device that is capable of storing digital information is a possible source of evidence in this regard. Not only does this include computers, both the desktop and laptop kinds, but also any handheld devices, servers, mainframes, video game consoles, digital video recorders, routers and firewalls, if the physical location

---

[43] Wortley & Smallbone 2006, p. 26.

[44] IP addresses are incredibly revealing, provided the suspect does not employ means to alter or hide his. Every IP can be looked up in one of numerous Whois-databases. This usually reveals the ISP that issued that particular address. From there, investigators can order the ISP to provide identifying details of their customer that was using that IP at a particular time.

has them present. Also, portable storage media such as burnt optical discs (CDs, DVDs), floppy and zip disks, backup tapes and memory cards and sticks have proven to be a valuable source of user files in the past. These media are usually not permanently connected to the computer, which means the chance that illegal files end up on them by accident is smaller.

Before sitting behind the computer and clicking through some random folders, however, investigators need to carefully search the premises for non-digital evidence. Regarding this, Ferraro and Casey make the valid distinction between the physical and digital crime scene.[45] The latter is situated inside the computer and its accessory sources of digital evidence, but the physical crime scene—the room or house where those digital sources are located—often contains much valuable evidence as well. Fingerprints on the keyboard and DNA samples around the room and on the chair, for instance, cannot necessarily demonstrate the possession of child pornography, but such evidence can be invaluable in proving who used the computer and thus needs to be collected. Additionally, investigators should document and photograph the scene.

Even after that, it is unadvisable to search the computer just like that. As outlined above, practically every single computer use is recorded, and everything that is recorded overwrites something that was recorded before. Essentially, even by just powering the computer up or pressing a random key, investigators could possibly overwrite valuable evidence. To counter this, the computer and all storage media should be seized and, in a dedicated lab, a bitstream copy of the storage media should be made. This involves connecting a separate computer to each particular medium, for instance the hard drive of the computer, to make an exact bit-for-bit copy of its contents. In contrast to searching the medium and copying just the files that are needed, a bitstream copy also includes all unused sectors and deleted files, which may be very relevant at a later stage in the investigation. If certain media cannot be seized, the copy can be made on site, but a search of the digital crime scene should always be conducted in a dedicated environment, and never on the original equipment.

Two fundamental principles must be adhered to when making a bitstream copy:[46] the copying process should not alter the original in any way, and the process should produce an exact copy. These principles can easily be protected in two ways. First, a write blocker device can be connected to the original storage media, to prevent any change to even a single bit of it. Second, the accuracy of the copy can be checked afterwards by means of a hash function: a unique identifier that is calculated both on the basis of the original medium and the copy. If the two identifiers match, the copy is proven to be exact.

---

[45] Ferraro & Casey 2005, p. 80.
[46] Mason 2007, p. 84.

A digital copy inherits all the shortcomings of the original digital evidence in that it is volatile and easily altered. For this reason, making multiple copies is sensible, preferably with multiple tools, since each might give slightly different results. Furthermore, investigators should use completely erased disks as the basis for the copies.[47]

On a side note, the expert literature is rather divided on whether or not to deactivate a computer if it is found switched on. Casey recommends turning it off.[48] He admits that some data (including the entire contents of the RAM, which might contain login passwords and similar data) will be lost, but consents that turning the computer off will guarantee the integrity of the evidence that is already present: the suspect might have rigged the computer to automatically delete certain files at certain times, and powering it down prevents this. For that matter, Casey recommends immediately unplugging the computer from the electrical outlet rather than powering it down the traditional way, since this traditional shutdown process might be rigged to delete evidence as well.

A good example of the evidence that is lost when the computer is powered down is found in the ongoing Dutch case of Robert M., in which police powered down the computer once they found it, immediately losing access to encrypted and/or hidden sections of the hard drives where many child pornography files are expected to be found. Dutch forensic experts, at the time of writing, still have a hard time opening those sections up again.[49] For similar reasons, in Mason's view, computers should be left on as long as possible.[50] The best compromise here might be to collect and copy RAM and other volatile data before taking the power down on the system.

3.2.3 Legal basis for investigating child pornography

The legal basis for search and seizure in Dutch law is to be found in the Dutch Code of Criminal Procedural (DCCP, *Wetboek van Strafvordering*). The Dutch legislation doesn't necessarily correspond to Casey's concept of the physical and digital crime scenes, in that there are no specific provisions on the search and seizure of computer data: the traditional provisions on search and seizure[51] can be used to seize entire computer systems and other storage media, after which investigators are free to examine them as any other piece of evidence. These powers require a warrant, usually from the prosecutor, except when catching the suspect red-handed,

---

[47] The suspect in the Dutch lower court case Rb. Breda, LJN AY5348 has argued, unsuccessfully, that the child pornography found on the copy of his hard drive was, in fact, left on the copy disk from a previous investigation.
[48] Casey 2004, p. 224.
[49] L. Essers, 'OM mist inzicht in encryptie Robert M.', Webwereld January 5, 2011, webwereld.nl/nieuws/105280/om-mist-inzicht-in-encryptie-robert-m-.html.
[50] Mason 2007, p. 46.
[51] Relevant search provisions include articles 96b, 96c, 97 and 100 DCCP. Seizure is regulated in 95, 96, 96a and 104 DCCP. See Koops 2010, p. 23.

which will of course rarely be the case with suspicion of possession of child pornography. A separate act called the General act on entry[52] requires an additional warrant for entry into a home, which is usually where evidence of child pornography is located. In order to be issued, these warrants require a reasonable suspicion of an offence.

The principles of proportionality and subsidiarity, largely unwritten[53] but notably present in the Dutch legal order, dictate that coercive powers are to be used in proper balance in relation to their goal. This means that investigators, although having the power to search and seize as much as they see fit as to not leave any evidence behind once a reasonable suspicion has arisen, they have to take care in not disrupting a personal life or business by taking as much digital devices as they can.[54]

Relevant ancillary powers include article 125k DCCP, which enables the investigator to order the undoing of security measures and decryption of encrypted data. Article 125j DCCP allows investigators to conduct a network search, from the premises where the computer is situated, to elsewhere-located computers that are normally accessible from this computer. A peculiar ancillary power is granted in article 125o DCCP, which allows investigators to prevent subsequent access to the original data by making it inaccessible. This includes deleting the data from the original computer. Of course, the use of this power destroys original evidence, so it should be used with caution. Conserving the original computer and preventing access to it by anyone serves the same purpose, but retains the evidence.

What's more, the Dutch legislation, by virtue of its wording, assumes that searches are conducted on the premises on which the computer is located. It should be noted here that this is in sharp contrast to taking the computer to a controlled environment, which most authors suggest.

The general police competence of article 2 of the Police Act is sufficient legal ground for investigators to search peer-to-peer networks and other services for offered child pornography.[55] In order for investigators to take part in child pornography-trafficking

---

[52] *Algemene wet op het binnentreden*, *Stb*. 94, 572.
[53] Principles of proportionality and subsidiarity are reflected in several provisions in Dutch criminal law, but never mentioned in so many words.
[54] This principle was seriously undermined in the lower court case Rb Maastricht 21 February 2008, LJN BC5445. The suspect's personal computer was seized because child pornography resided on the hard disk, but he needed that computer in his international marketing consultancy business. The court politely refused, stating that the computer needed to be seized because data cannot exist on its own. It acknowledged that data can be copied to separate media 'nowadays', but whether or not investigators do so is up to their discretion and the interests at hand.
[55] Oerlemans 2010, p. 76.

Usenet or newsgroup,[56] the more stringent articles 126j DCCP (undercover operations) and 126h DCCP (infiltration) come into play.[57]

A great many provisions in the DCCP are related to production orders and preservation of data. In relation to Internet crimes such as accessing child pornography, these might uncover valuable information if directed to the suspect's ISP. They include art. 126n for the production of traffic data; 126nc for user data; and 126ni for the preservation of certain volatile data.

3.2.4 The investigative process

Once the suspected storage media are copied and ready to be analysed in a dedicated laboratory, digital investigators are ready to search the bitstream duplicates for any traces of possession of child pornography. First and foremost, it must be noted that investigators need to extensively document the process, to the extent that a different investigator can replicate the investigation with the same results. This document file will be available to all parties in the case, and the entire analysis procedure might be questioned in court.

Randomly clicking through some folders in the hope of finding child pornography is usually not the best way to go about the search. Although some suspects might keep their illegal files in an easily accessible place in their file system, many child pornographers are more calculating and hide their collection one way or another, in order to avoid detection. This means investigators need to employ more organised procedures for scrutinising storage media.

Several software solutions, the most famous of which is EnCase,[58] can be used for assistance and automation of the digital forensics process. Connected to the evidential storage medium, these solutions allow investigators to easily recover files and find evidence, and their use has generally been accepted as providing reliable results. To successfully use them, these tools do require extensive training and even certification. Also, although this software automates much of the process, investigators should still know the nuts and bolts of manually investigating a storage media, should the need arise to investigate beyond what the program is capable of doing or it displays some sort of flaw. For that matter, Casey recommends carrying out the same investigation more than once, using different software tools, to increase the chance of accurate findings.[59]

Investigation should typically be conducted on a dedicated computer that is not connected to the Internet, to exclude the possibility of outside interference in the investigation.

---

[56] Koops 2010, p. 28.
[57] Oerlemans 2010, p. 79.
[58] www.guidancesoftware.com.
[59] Casey 2004, p. 264.

3.2.5 Recovery of files

The first step in analysing seized storage media is to open up access to all the files on them. Probably the easiest files to regain access to in this regard are deleted files. When a computer file is deleted (and subsequently removed from any intermediary recycling bin), only the file system reference to that file is deleted—the actual contents of the file remain on the hard drive, inaccessible and ready to be overwritten. Casey draws an analogy with a library that has a card catalogue of its contents: if a card for a specific book is removed from the catalogue, the book remains on the shelf—it's just that nobody knows it's there. Searching the unallocated space and slack space of storage media, investigators can, often quite successfully, recover much deleted data.[60]

Encrypted files are more troublesome. File encryption is the process of taking an intelligible file of any type and scrambling its contents, seemingly randomly, but in fact based on a mathematical function that works on a unique key. The result is an unintelligible assortment of bits on the storage medium: only by inputting the key and running the process in reverse (called 'decryption') can the file become intelligible again. Of course, this key is a password that is usually only known to the suspect, and the coercive power of ordering a decryption key cannot be directed towards him,[61] because of the privilege against self-incrimination.

There are other ways of getting the encryption key, with varying degrees of success. Sometimes, the suspect has written the key down on handwritten notes or other scraps of paper, lying around his computer.[62] Guessing the password has a very low potential, but investigators might get lucky. A so-called cold boot attack has had some success in breaking encryption, but has to be performed on the original computer and storage medium, a method that is at odds with the principle of original data preservation. As a last resort, brute force methods can be used to crack the encryption. Essentially, this involves trying every single possible key, and while this has been successfully carried out in the past for simpler keys of up to 128 bits, freely available encryption software such as TrueCrypt supports keys of up to 256 bits. Each additional bit doubles the amount of possible keys and thus doubles the workload to break the encryption. If it would take a computer an hour to find the password for 128-bit encryption, that same computer would need countless millennia to find the 256-bit key. Such keys can simply not be cracked by currently available computing power in a feasible amount of time and, once again, the privilege against self-incrimination prevents investigators from obtaining the key from the suspect.

---

[60] Whether or not the suspect can still be said to possess the images (or possibly possessed them in the past) if they were found as deleted files on his hard drive is a legal matter for the court to decide. More on this in the next chapter.
[61] Article 125k, section 3 DCCP.
[62] Ferraro & Casey 2005, p. 175.

3.2.6 Finding evidence

Once all recoverable files have been retrieved, investigators are left with hundreds of thousands of files to scrutinise for evidence of child pornography. Usually, some form of data reduction is in order. A large portion of the files on hard disks are known system files, such as those from the operating system and installed programs on the computer. Using a hash function to identify them, these files can then be removed.[63] Theoretically and in the best-case scenario, this leaves only unknown and user-created files on the medium. Data reduction is a good way to reduce the workload of searching though immense amounts of files, but investigators should take care not to get overenthusiastic with deleting data; some useful evidence might get thrown out accidentally.

At this point, investigators may start the actual process of searching for evidence of possession of child pornography, that is to say, child pornographic images or traces thereof. These images can be located in and should be searched for in user file folders, through system and program files, and in temporary files and cache files.[64] However, by only searching for image file types—particularly JPEG files—or keywords, investigators might overlook much evidence. The suspect could have simply given his image files a different extension, or used more advanced techniques, such as embedding them into other files[65].

The software packages that investigative agencies typically use allow the investigator to scrutinise the storage medium for file headers.[66] These headers are unique to each file format and, regarding image files, contain such information as the size, resolution and the colour depth of the image. Essentially, wherever image header data has been located on the storage medium, an image has been found.

Another often-used method is a search for illegal files based on hash functions. Instead of assessing every individual image file on the storage media (possibly hundreds, if not thousands of files), investigators can generate a hash function of every image file on the medium and compare these functions to a database of functions of known child pornography files. If a match turns up, a child pornographic image has been found. This investigative method has the benefit of speed but carries a risk of missing evidence when the suspect has altered the files in some way[67] or, once again, embedded them into other files. Also, the use of hash functions to

---

[63] Casey 2004, p. 110.
[64] Mason 2007, p. 9.
[65] For instance, using some simple, readily available software tools, any file can be hidden inside a JPG file: lifehacker.com/#!282119/hide-files-inside-of-jpeg-images.
[66] Casey 2004, p. 230.
[67] Even the slightest of changes in a file will generate a dramatically different hash function.

identify files is not without controversy, as some dispute the uniqueness of these functions.[68]

Please note that most jurisdictions differ in their definitions of which material is to be considered child pornography and thus criminal. A framework decision of the European Council has made some effort to streamline this among its Member States.[69] Although an important matter in itself, this thesis will not go into further into the matter.

3.3 Evidence of intent of possession

3.3.1 Circumstantial evidence

Finding images of child pornography on a storage medium confirms criminal activity. All that remains is finding the person responsible for placing them there. The owner of the computer is usually a good start, but not necessarily the guilty individual. Perhaps more people use the same computer or have access to it. The computer could be an office machine to which co-workers have access, or it could have been obtained second-hand from the previous owner. The user could have accessed an innocent-looking website, but was surprised to find child pornography there (inadvertently downloading those images automatically by means of the browser cache). Indeed, it could very well be possible that a stranger across the world remotely placed the images on the computer, or malicious software automatically downloaded it. Investigators need to be aware of these possibilities and look into their likelihood.

In the Netherlands, the test that judges utilise to determine whether or not a suspect can be said to possess images on a computer is the following: criminal liability exists if the suspect is "aware of the presence of these files, has power of disposal over these files, and has the intention of possessing them."[70] Additional evidence should thus focus on the aspects of awareness, control and intention.

First of all, the suspect may be perfectly willing to explain if and how he obtained the images. Additionally, his relatives and contacts may provide statements on the suspect's sexual interests and activities.[71] When this is not the case, investigators have to look for other circumstantial evidence to prove awareness, control and intention.

---

[68] See www.dfrws.org/hashchallenge/index.shtml.
[69] EU Framework Decision 2004/68/JHA.
[70] Stevens & Koops 2009, p. 12: "Degene op wiens harde schijf kinderporno is aangetroffen, is strafbaar wegens het opzettelijk in bezit hebben van deze kinderporno, indien hij zich bewust is van de aanwezigheid van de bestanden, hierover beschikkingsmacht heeft, en de bedoeling heeft ze in bezit te hebben." Translation by Koops in Koops 2010, p. 16.
[71] Ferraro & Casey 2005, p. 249.

Metadata of the child pornography images, particularly their time and date stamps, are a critical factor in this. These stamps reveal the exact date and time the images were placed on the storage media (which generally corresponds to the time they were downloaded), and, more importantly, when the files were last accessed. By creating a temporal reconstruction of the events around that time, investigators can deduce who was using the computer at that moment in time, and how he was using it. Carney and Rogers, based on a short experiment, established it to be quite possible to determine the origin of a file based on time stamps.[72]

However, the time stamp evidence does not rule out the possibilities of malware or remote downloading. The temporal analysis might bring to light malicious software at work, when the time stamps show, for instance, that child pornographic websites were accessed 40 times in one minute.[73] Note that time stamps can also be altered, as a simple Google search reveals, although these changes might be tracked by the operating system or otherwise spotted by investigators when compared to other log files.[74] Because time stamps rely on the computer's system clock, investigators need to make sure this clock runs punctual or offset the stamps accordingly.

Further evidence that increases the certitude of a suspect having awareness, control and intention can be found in system, application and network log files. As outlined above, these logs retain particular details on computer usage. Reconstructing the log entries into a temporal analysis can show how the computer was used during a period of time. For instance, network logs might show a certain connection with an IRC channel, and the application logs from the IRC chat client program can show that, in the course of that connection, certain child pornography files were transferred to the computer. Once again, this evidence is not conclusive: these logs can also quite easily be tampered with but, combined with correlating circumstantial evidence, there might be enough for a conviction.

Finding the child pornographic images, or duplicates thereof, on separate storage media is a very strong indicator towards awareness, control and intention. These sources include optical disks and external hard drives that are not permanently connected to a computer, and thus there is a reasonable probability that the suspect wilfully put or copied the images onto those media.[75]

A functional analysis might bring to light different aspects of the case.[76] Using this type of analysis of the computer, investigators compare the evidence to what the computer is technically capable of. Consider this example: evidence logs show that certain files were copied to a USB flash drive at a certain time, but the computer does

---

[72] Carney & Rogers 2004.
[73] As were the circumstances in the case of Michael Fiola, explained in the previous chapter.
[74] Ferraro & Casey 2005, p. 285.
[75] Ferraro & Casey 2005, p. 154.
[76] Mason 2007, p. 17.

not have any USB connectivity ports. Contradicting evidence like this is a good indication that something peculiar is going on.

Additional locations for circumstantial digital evidence that supports charges of possession of child pornography include the Windows registry, where certain login credentials are saved; the pagefile or swap file (depending on the computer's operating system), where evidence of accessed files and programs may reside; references to the images in the Windows Recent folder or operating system-generated thumbnails of those images (demonstrating that the files have been opened at least once)[77]; and browser cache, history and cookies, uncovering which websites have been accessed. Once again, none of these are conclusive in and of themselves since they can be modified, but enough of this corroborating evidence increases the probability of intent.

3.3.2 Data fabrications and other excuses

No awareness, control and/or intention exist when the illegal images ended up on the suspect's computer without his consent. Defences in this regard are numerous but courts rarely accept them. However, it has been demonstrated in the previous chapter that there is indeed a possibility of malicious software directing images onto a computer without its owner being aware of the data. Citing Ferraro and Casey; "Investigators, prosecutors, and forensic examiners should rule out the virus defense before proceeding with a case because it is sometimes plausible."[78]

How can these defences be ruled out? As it turns out, remote access to a computer, either through a direct connection or through the use of malicious software such as Trojan horse programs, leaves traces of itself.[79] Off-the-shelf computer security programs can find most malicious software, and remote access to a computer will usually leave an entry in a network log. Of course, more sophisticated hackers[80] can wipe traces of their activity, and particularly effective malware hides itself from view. No traces of malicious activity does not exclude the defence so, once again, additional corroborating evidence is needed for greater certainty, for instance from the suspect's ISP, which might hold records of connections the computer made.

3.4 Evidence of accessing child pornography

When investigators cannot find child pornographic images in the possession of the suspect, criminal liability may still exist when it can be evidenced that the suspect

---

[77] Carney & Rogers 2004, p. 4.
[78] Ferraro & Casey 2005, p. 280.
[79] Ferraro & Casey 2005, p. 248.
[80] The term 'hacker' is used here in a nonspecific sense as any person purposefully gaining access to a computer that is not his own, either remotely or physically, directly or with the use of malicious software.

accessed child pornography in one way or another. Or, to turn matters around, investigators do not *need* to find child pornographic images, since proving access to it will result in the same theoretical[81] degree of criminal liability, at least under the recent addition to existing Dutch criminal law.[82] Either way, investigators would do well to extend their analysis of the suspect's computer to include evidence of access to child pornography. The gathering procedure for this evidence follows the same rules as above, but the actual evidence might be different.

The most uncomplicated example of such evidence would be an entry in the browser history of a known child pornographic website. Although valid evidence, it is unrealistic to think it will be regularly found, given the rarity of websites on the 'open' Internet[83] where child pornography is freely available, and relative easy ways around keeping automatic history for browsing sessions.[84] Investigators will likely have to turn to other sources.

Further evidence of child pornography access could possibly include records of credit card or other payments for specified services relating to child pornography, login credentials to such services that are stored on disk or written down on a scrap of paper, and computer log files that show access to these services. Needless to say, not all child pornography is paid for, and not all access requires login credentials. Ultimately, ISPs might be the best provider for detailed information: they keep detailed information logs on what was accessed by whom, based on user IP address.[85] In his extensive analysis, Ohm asserts that ISPs have a unique broad perspective of *almost all* Internet activity of their customers,[86] plus the possibility to zoom in on individual activity for a deeper view. As a matter of fact, ISPs possess only two 'blind spots': they cannot view encrypted data, and they do not have access to customer data of other ISPs.[87] Of course, the latter is no hindrance to investigators into child pornography, since they have access to customer data from all ISPs, of which there is always one involved.

Art. 126ni DCCP can be used to order the preservation of online user activity. Legal sources on this provision remain vague as to exactly *which* information can be

---

[81] Theoretical, because criminal sanctions in the Netherlands denote only a maximum; the actual sanction is left to the discretion of the judge. Since, at the time of writing, not one person has been convicted for accessing child pornography, it is as of yet unknown whether or not courts will impose similar sanctions.
[82] See section 2.1 for the review of the specific provision.
[83] As compared to the 'hidden' Internet.
[84] Most modern web browsers have a 'private browsing' function (often called 'porn mode', tongue-in-cheek) which deactivates browser caching and history keeping for the duration it is switched on.
[85] Ferraro & Casey 2005, p. 86.
[86] Even more so than for instance Google, a company often criticised for the amount of private information they allegedly collect. See Ohm 2009, p. 28.
[87] Ohm 2009, p. 26.

ordered for preservation[88], but given the theoretical ability of ISPs to monitor all user activity explained above, it might be assumed this provision could assist in investigating the offence of accessing child pornography.

Having said that, investigators have to take care not to get overzealous in finding evidence of accessing. The Dutch legislator acknowledged the possibility that such traces might end up on a computer by misfortune.[89] Therefore, as is the case with possession, the offence of accessing child pornography equally requires criminal intent on that access: accidental access, for instance by unsuspectingly following an innocently labelled hyperlink, should not be criminalised. In the words of Koops, "evidence should show that the defendant was actively focusing on accessing child pornography".[90]

Stevens and Koops, in a critical view on the provision, challenge the usefulness of the addition. They conclude that less technologically developed child pornographers will have a hard time *not* leaving any images behind (meaning they can be charged with possession proper), whereas more tech-savvy suspects—those that can prevent or wipe traces of possession of images—should have no problem covering their traces of access. They observe that only in a small number of specific cases will the provision extend criminal liability.[91]

3.5 Digital forensics best practices guidelines

3.5.1 International guidelines

Many organisations and working groups over the years have come up with guidelines. These are usually directed towards law enforcement, prosecutors and—to a lesser extent—private investigators, and mostly consist of a detailed explanation of the implications and intricacies of digital evidence and the best practice for collecting and analysing it. The organisations and their guidelines include the following:

- The Scientific Working Group on Digital Evidence[92] (Best Practices for Computer Forensics[93])
- UK Association of Chief Police Officers[94] (Good Practice Guide for Computer-Based Electronic Evidence[95])
- Executive Office for US Attorneys[96] (Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations[97])

---

[88] See, for instance, Cleiren & Nijboer 2009.
[89] *Kamerstukken II* 2008/09, 31 810, No. 3, p. 4.
[90] Koops 2010, p. 16.
[91] Stevens & Koops 2009, p. 15.
[92] www.swgde.org.
[93] www.swgde.org/documents/current-documents/.
[94] www.acpo.police.uk.
[95] www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

- US Department of Justice (Child Pornography on the Internet,[98] in the Problem-Oriented Guides for Police/Problem-Specific Guides series, and Office of Justice programs, such as Forensic Examination of Digital Evidence: A Guide for Law enforcement[99])

For the most part, these guidelines all consist of recommendations. They do not impose any binding procedures on investigative agencies; rather, they suggest what they consider to be best practice consensus in digital evidence approaches. This is explained for instance in the Forensic Examination of Digital Evidence guide, stating that the guide's recommendations are certainly not feasible in all situations and do not represent the only appropriate course of action.

3.5.2 Dutch digital forensic procedure

The lack of a best practice consensus that applies in *all* situations is precisely the reason why there are no digital evidence guidelines in the Netherlands, according to the interviewed investigators. The process of digital investigation is too changeable and too intensely subjected to technological developments to plan out in general regulations. For some individual operations, such as the copying of a hard drive, FT-norms[100] are in the works to streamline the process, but a guideline with any larger scope than that is non-existent. This is not to say that digital investigation is random and disorganised: the Digital Expertise teams throughout the country have all sprung from the same national project in the 1990s and have thus all adopted the same working methods.

The teams maintain close contact on new developments and cases, and continue to work together on all matters regarding digital evidence. Of particular interest is the National Database Child Pornography that digital expertise teams have started to employ in recent years.[101] Every single child pornographic image that is found during investigation is added to this database, with the goal of establishing a never-ending collection of every known image. By automatically calculation of hash values, investigators can easily compare the yield of their current investigation to the hash values of the images in the database and, by virtue of the fact that these values are

---

[96] www.justice.gov/usao/eousa/.
[97] www.cybercrime.gov/ssmanual/ssmanual2009.pdf.
[98] www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.
[99] www.ncjrs.gov/pdffiles1/nij/199408.pdf.
[100] Forensic-Technical norms. These are procedural guidelines drafted by technical investigators, working groups of the Dutch Forensic Institute and other experts, and provide requirements and recommendations for discovering and securing evidence. See the Factsheet FT-norms, available at www.fomat.nl/nfi_fsnormen.pdf.
[101] *Landelijke Database Kinderporno*. See http://ziuz.com/nl/landelijke-database-kinderporno.ashx.

unique,[102] establish possession of child pornography without ever looking at the material.

Some rudimentary regulation of the investigative process does exist. There is an Instruction child pornography (*Aanwijzing kinderpornografie*)[103] that predominantly deals with the criteria of which images are to be considered child pornography, and it summarises the coercive means that are available to investigators in case of suspicion of child pornography. Interestingly enough, the instruction requires police teams that deal with child pornography investigations to draft more specific guidelines for digital forensic procedure—to no effect, as of yet.

The instruction acknowledges the significance of specialist digital investigators in pertinent cases, but it does require a vice detective to be involved in the investigation in three specific situations: search and seizure of illicit material should take place under the supervision of a vice detective; interrogation of witnesses, victims or the suspect should be performed by at least one vice detective; and assessment and classification of seized material is the sole responsibility of these investigators.

The instruction also stresses the importance for investigators to seize *all* data carriers of the suspect. Investigators of digital expertise must be present during a search and seizure. Furthermore, it recommends investigators to photograph the various rooms of the residence. These can later be compared to any child pornography images or videos found, in order to determine possible child pornography production by the suspect. It goes on saying that the seized material is to be treated with the utmost care and should be registered. In order to determine the unlawfulness of the material, a vice detective should carefully and manually analyse the material: a positive match to a reference database is not enough for evidentiary value.[104]

The Guideline child pornography (*Richtlijn kinderpornografie*)[105] expands on the instruction, mainly by providing a table of sentence indications based on particularities of the case at hand.

Although not specifically dealing with child pornography, the Instruction technical investigation/specialist investigation (*Aanwijzing technisch onderzoek/deskundigen-*

---

[102] Some authors debate the uniqueness of hash values. Although there are billions of possible values, a typical hash is 'only' 32 bytes long, whereas a computer file can have a practically unlimited number of bytes. There are always more possible files than possible hash values, so inevitably, one hash applies to a multitude of files. Furthermore, the algorithm for creating hash values is believed to have been cracked, possibly decreasing their evidentiary value. See www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202475161643. Evidentiary value of hashes is discussed in more detail in the next chapter.

[103] *Stcrt* 2010, 19121.

[104] As based on HR 1 July 2008, LJN BC8645. This will be discussed in more detail in the next chapter, when discussing the charges.

[105] Available at www.om.nl/organisatie/beleidsregels/overzicht/zeden/@155136/richtlijn/.

onderzoek)[106] is of importance. It specifically states that in *all* cases in which the investigation will irreversibly alter the crime scene, investigators are to inform the prosecutor, who will decide on whether or not to involve a specialist into the investigation. This is important with respect to certain rights the defence has with respect to specialist investigation. Subparagraph 4.3.5 will deal in more detail with specialist investigation and its relation to technical investigation. Of course, as evident from the above overview, digital forensic investigation is hardly, if at all, destructive, so it can be gathered that specialists are rarely involved in this type of investigation. In fact, the instruction later goes on to state that certain categories of investigation, when conducted by investigative authorities, are to be excluded from specialist investigation.[107] The area of information technology is on that list. This leads to the conclusion that at least during the preparatory investigation, involvement of specialists is non-existent and the entire investigation is conducted by technical investigative authorities. As will be shown in the next chapter, specialists are not entirely off side though, particularly in the courtroom.

---

[106] *Stcrt*. 2009, 18632.
[107] Also see *Kamerstukken II* 2006/07, 31 116, nr. 3, p. 10 and Keulen et al. 2010, p. 55.

4 DIGITAL EVIDENCE IN COURT

4.1 Criminal charges

At the end of the preparatory investigation, if the prosecutor deems a conviction likely, based on the evidence that has been accumulated thus far, the suspect is charged with possession of and/or accessing child pornography.[108] Evidence, according to Nijboer, has the function of asserting the validity of a certain hypothesis.[109] The criminal charge can be considered such a hypothesis in a legal sense, in which case the evidence resulting from the forensic procedure is used to test that conjecture. Judicial evidence exists in relation to something—something that has to be proven, something which Nijboer designates the *probandum*.[110] It's the prosecutor's job to create this probandum, by means of charging the suspect with the alleged criminal offence, outlined in a clear description that the suspect can understand and the judges can use as a basis for the investigation at trial.[111]

Stevens and Koops have made an extensive catalogue and analysis of child pornography cases, in order to research the exact judicial standing towards the requirements for conviction, in particular the required intent. They concluded that a suspect is criminally liable for intentional possession of child pornography if he was aware of the presence of the files, had control over them, and meant to possess them.[112] Evidence from the preparatory investigation thus has to focus on proving those criteria.

4.1.1 Charging for possession

The Dutch Supreme Court requires charges to be sufficiently factual, and has ruled that the words "sexual act" in article 240b DCC do not meet that criterion.[113] Including the actual images in the charge is obviously not an option. The solution that prosecutors have come up with and, more importantly, courts have accepted, is to describe in general the extent and nature of the collection of material that was found, and describe in detail a small selection of no more than 25 images and/or video files to be included in the charges. This selection is understood to be representative for

---

[108] *Usually*—the principle of opportunism (laid down in articles 167, section 1 and 242, section 1 DCCP) leaves it up to the prosecution's discretion as to which offences and felonies to prosecute, regardless of the amount of incriminating evidence. Still, there are policies in place that regulate this discretion, and prosecution of child pornography is particularly high up on the priority list.
[109] Nijboer 2011, p. 19.
[110] Nijboer 2011, p. 19.
[111] See article 261 DCCP and Nijboer 2011, p. 160.
[112] Stevens & Koops 2009, p. 12.
[113] HR 28 September 2004, *NJ* 2004, 684.

the entire collection. The prosecutor is supplied with a hardcopy of the actual images of the selection, to present at trial, but these are not included in the case file and are not available to anyone other than the prosecutor.[114]

The National Database Child Pornography[115] creates the potential for charging suspects for possession of child pornography based exclusively on hash values matching those in the database. However, the Dutch Supreme Court rejected this practice, concluding that an investigative report solely stating that the images on the suspect's computer match those of the database is not enough to support charges. Evidence requires more than just the positive match, according to the Court: the status of the database and the criteria for including images into it will have to be made sufficiently clear.[116] As of yet, investigators are eagerly awaiting a prosecutor to once more test this practice in court, seeing that it would make their investigation significantly less demanding—particularly because the respective vice officer would no longer have to view so many images of child pornography in his assessment.

4.1.2 Confiscation

The Instruction child pornography is particularly clear on the fate of the seized data carriers that contain child pornography: at trial, the prosecutor should always appeal for confiscation of those items and they should be destroyed as soon as a positive peremptory court decision is established. This means that a data carrier containing child pornography will never—*ever*—be returned to the suspect, despite any personal or business-related files that might be on there. Digital investigation cannot guarantee that all illicit material has been found and erased from the data carrier. Some illegal files may be hidden or inaccessible and can therefore not be evaluated by investigators. Finally, erasing files is never foolproof, and some (or even all) of the erased files may at a later date be retrieved. Furthermore, the practice of erasing and returning files would shift the police responsibility into that of a copy facility, which is even more undesirable. The only way to make sure these illegal files are not returned into society is to destroy the data carrier. The instruction considers this to be the suspect's risk: by involving himself with child pornography, illegal and non-illegal data become mixed.[117]

According to the interviewed investigators, sometimes digital investigators nevertheless return certain files to the suspect or his family members off the record—for instance the school essay of the suspect's son.

---

[114] *Aanwijzing kinderpornografie*, p. 7.
[115] The database allows investigators to assess images without ever looking at them, by means of their hash values. See subsection 3.5.2.
[116] HR 1 July 2008, LJN BC8645.
[117] *Aanwijzing kinderpornografie*, p. 8.

4.2 Law of evidence in the Netherlands

4.2.1 The investigation at trial

In a nutshell, the preparatory investigation's purpose is to gather enough material to clear up the case and to have the prosecutor make an educated decision on whether or not to charge the suspect. Subsequently, the investigation at trial is meant to decide on the validity of that material and evaluate whether or not a conviction can be founded by it.[118] What follows in this paragraph is a brief, general overview of the particularities of Dutch procedural law and law of evidence with regard to child pornography cases.

Judges in Dutch criminal proceedings are traditionally considered to be inquisitive,[119] meaning that they have an active investigative role during the investigation at trial. Though the judge, like the suspect, is limited to the criminal charges as far as his investigation goes, within that framework he is free in the selection and evaluation of that material with regard to a conviction[120] and can add to or discharge the results of the preparatory investigation (article 315 DCCP). It is the judge's active task to examine everything that is put forward at trial, so as to get a clear picture of what exactly transpired with regard to the criminal offence that the suspect is charged with.[121]

As a consequence of the positions of the judge, the prosecution and the suspect in Dutch criminal proceedings, there is no strict division of the burden of proof between the suspect and the prosecutor in Dutch criminal proceedings.[122] Some say that, if there is any burden of proof at all, it is on the court, because of its inquisitive role in the process.[123] Others are of the opinion that the burden of proof is on the prosecutor: he is expected to present the evidence that supports the charges.[124] Still others argue that there is a *negative* burden of proof on the suspect, to the extent that certain articles of evidence can be used if the defence does not complain about them,[125] or even a *positive* burden because criminal culpability is often assumed if there are no contradictory indications, and it is up to the suspect to prove otherwise.[126] Although it is the judge's duty to be mindful of any exculpatory information regardless of what the suspect does or does not share, the judge (or

---

[118] Nijboer 2011, p. 69.
[119] Nijboer points out an ongoing development in the Netherlands in which judicial duties and obligations throughout the proceedings are becoming slighter although, according to him, the inquisitive judge is still responsible for the complete and correct investigation at trial. See Nijboer 2011.
[120] See below under 4.2.2.
[121] Nijboer 2011, p. 154.
[122] Nijboer 2011, p. 30 and p. 159.
[123] Van Kampen 1998.
[124] Van Koppen 2011, p. 28 and Nijboer 2011, p. 160.
[125] Broeders 2003, p. 73.
[126] Nijboer 2009, p. 47.

indeed the prosecutor) cannot and is not expected to know specific information only the suspect has knowledge of.[127] As will be evident from the discussion below, some—if not all—of those elements can be found in the criminalisation of child pornography.

All information on which the conviction is based has to be put forward during the investigation at trial: this investigation is required to be 'complete.'[128] The judge might be withheld possible relevant information because expert investigators of police or the prosecution fail (intentionally or not) to report non-inculpatory or even exculpatory evidence—something that does indeed happen in practice, according to Broeders, because such evidence is on occasion considered to be 'irrelevant' by investigators. He goes on to say that the defence has to explicitly request results of conducted research that was not reported in order to acquire insight into this investigation.[129] However, first and foremost, the completeness of the investigation is the judge's responsibility, as evident from his duty to order more in-depth investigation if some evidence remains unclear (articles 315–318 and 346–347 DCCP).

4.2.2 Admissibility of evidence

The prosecutor can present any and all of the findings of the preparatory investigation at the investigation at trial for the judge to consider,[130] making all evidence admissible, effectively. Those results do not become evidence in the judicial sense of the word until the judge can (and will) fit them into one of the categories of article 339 DCCP to support his conviction, but the prosecutor is free to put them forward nonetheless. Ultimately, the judge is free in selecting and evaluating that material with regard to his conviction,[131] although some rules limit the free selection and evaluation of evidence, because certain types of evidence were though by the legislator to be unreliable or unwarranted from the outset.[132]

The negative-statutory system of evidence[133] means that a conviction may only be based on the types of evidence in the list of article 339 DCCP, and that the judge must obtain the personal conviction of the suspect's guilt, irrespective of the amount of admissible evidence against him.[134] The limited system ensures that only evidence that was acquired in accordance with the investigation regulation will be used as foundation for the conviction.

---

[127] Nijboer 2011, p. 75 and p. 164.
[128] Article 338 DCCP. See also Nijboer 2011, p. 65.
[129] Broeders 2003, p. 90. This is perfectly in line with his view of the negative burden of proof on the suspect.
[130] Broeders 2003, p. 72 and Van Kampen 1998, p. 312.
[131] Nijboer 2011, p. 70.
[132] Nijboer 2011, p. 59.
[133] See Corstens 2008, p. 665.
[134] Corstens 2008, p 666. The system is nuanced by case law, such as the exclusion of evidence that was obtained unlawfully (HR 26 June 1962, *NJ* 1962, 470 (*Bloedproef II*)).

Nijboer argues that, although the regulation in the DCCP can be interpreted in multiple ways, the requirement of a sound investigation in criminal cases dictates that conviction cannot be rooted on a single piece of evidence.[135] He calls this the requirement of *double affirmation*: there is always[136] a multitude of sources of evidence required for a conviction.[137] It is important to note that this does not mean that every isolated element of the charges has to be covered by more than one item of evidence; the Dutch Supreme Court has accepted (some 80 years ago) a construction in which one item of evidence covered the entire charge and a second item covered a minor part of the charge.[138]

4.2.3 Judicial conviction and justification[139]

Although judicial conviction is, in essence, a personal matter for the judge to decide on, some authors have tried to elucidate when, exactly, the judge can consider himself to be convinced. Nijboer reckons this to be the case when there is an *indication of a highly pressing degree of probability*.[140] If the correctness of the charges follows from the available evidence '*beyond reasonable doubt*', the judge can be considered convinced,[141] especially because, as Casey puts it, "in forensic science, certainty is impossible."[142] The result of the investigation at trial—the judge's decision—is asymmetrical in that any reasonable doubt is to the advantage of the suspect.

The judge's personal conviction has to be evident from the justification: the correctness of the conviction must be 'beyond reasonable doubt' solely based on the grounds of that justification; there should be no internal contradictions;[143] and any alternate explanations should specifically be excluded. The judge may ignore extremely unlikely scenarios,[144] although ever since the recent update of article 359, section 2 DCCP with respect to justificatory requirements, he is obliged to state

---

[135] Nijboer 2011, p. 76. Casey shares this opinion with regard to digital evidence, because of its circumstantial nature. See Casey 2004, p. 17.
[136] An exception applies: conviction may hinge on a single investigative report (as stated in article 344, section 2 DCCP), although in practice, this is only applied to simple offences or minor felonies. See Nijboer 2011, p. 76.
[137] Nijboer 2011, p. 77. Note specifically that a multitude of *sources*, not a multitude of evidence is required. Two articles of evidence from the same source are not sufficient when adhering to this rule.
[138] HR 8 June 1931, *NJ* 1932, p. 1550.
[139] The Dutch word *motivering* used in the DCCP is often translated with the English *motivation*. I believe this to be an incorrect translation. The English word *motivation* only covers one meaning of the Dutch polyseme *motivering*. The other meaning—the one used in this context—is better translated with *justification*, in the sense of "provide reasons for".
[140] Nijboer 2011, p. 73.
[141] This notion of 'beyond reasonable doubt' is precisely the standard of judicial conviction that dominates most common law jurisdictions.
[142] Casey 2004, p. 21.
[143] Nijboer 2011, p. 238.
[144] Nijboer 2011, p. 134.

reasons for refuting any *explicitly substantiated standpoint* of both the prosecution and the defence.[145] The Dutch Supreme Court, in a case following this addition to the legislation[146] explicated on this judicial requirement: the standpoint has to be put forward plainly, substantiated by reasoning, and accompanied by an unambiguous conclusion. The extent of the duty to respond depends on the nature of the subject matter and the degree to which the judge deviates from the expressed standpoint, according to the Court.

4.2.4 Facts of common knowledge

Facts of common knowledge do not require evidential foundations, as stated in article 339, section 2 DCCP. Which facts are considered to be of common knowledge very much depends on time and place: what is considered to be expert knowledge at one time can become common knowledge later on.[147] Ultimately, it is up to the judge to decide what is common knowledge and what is not.

Although these facts do not require specific evidential foundation, they should not be undisputable: it should always be possible, particularly for the defence, to contradict these facts. This alleviation of the evidence requirement should not be used to circumvent evidential problems.[148]

4.3 Evidence for child pornography

4.3.1 Digital evidence in Dutch courts

Pijnen and Fennell-van Esch wrote on the admissibility of digital evidence in the Netherlands, stating that all types of electronic evidence are, in principle, admissible. [149] As noted above, however, the prosecutor in Dutch criminal proceedings is free to present *any* evidence: *all* evidence is admissible in that sense, a fine distinction the two don't seem to make. Nonetheless, they are correct in that, even though digital evidence is not mentioned in article 339 DCCP, the Dutch Supreme Court has established in a 1996 case that it can, in fact, support the judicial conviction that article 338 DCCP requires.[150] As long as the particular evidence can be made to fit into one of the five categories of article 339 DCCP, the judge is allowed to use it for his conviction. It will usually end up in the category of written records, as will be apparent from the analysis below.

---

[145] According to Nijboer, the judge may still disregard only extremely unlikely possibilities. See Nijboer 2011, p. 134.
[146] HR 11 April 2006, *NJ* 2006, 393.
[147] Nijboer 2011, p. 85.
[148] Nijboer 2011, p. 209.
[149] Pijnen & Fennell-van Esch in: Mason 2008, p. 644. Nijboer (Nijboer 2011, p. 64) goes so far as to say that the current regulation is old-fashioned.
[150] HR 7 May 1996, *NJ* 1996, 687.

Extraordinary cases with plain and grave judicial errors regarding digital evidence, such as that of Matthew Bandy,[151] have fortunately never occurred in the Netherlands. Still, as will be demonstrated below, judges have—in a small number of cases—an uncertain way of dealing with digital evidence and, more importantly, with technical defences of the suspect.

4.3.2 Case catalogue

Stevens and Koops have made an extensive catalogue of defences in child pornography possession cases, in order to research the exact judicial standing towards the required intent.[152] Published in 2009, their research covers developments up until April of that year, and provides a good starting point for an in-depth analysis of judicial approaches towards digital evidence and defences. Additionally, the Dutch *Raad voor de Rechtspraak* (the judicial body that oversees all courts) started PROMIS[153], a national project to improve justification in judgments by explicitly requiring courts to explain their judgments and respond to all involved parties, in 2004. The project is an ongoing success and has resulted in more detailed judgments, particularly with respect to the evidence.[154] As such, the PROMIS judgments[155] have been a primary source in the analysis for this chapter, mostly because their detailed justification and explanation of the evidence used provides a detailed insight into judicial reasoning.

What follows is an analysis of the various means of evidence judges have used in cases of possession of child pornography, ordered in line with the statutory evidence categories of article 339 DCCP. Of those, the witness testimony will not be covered since its use always depends on specific circumstances of the case (such as an acquaintance or family member of the suspect being relevant to the investigation).

The criminalisation of access to child pornography has not led to a conviction yet. A recent case[156] has come quite close: the suspect admitted he had accessed child pornographic websites from his work computer, but he did not download or otherwise tried to possess any images. Although images were found in his browser cache, the court could not assume the suspect had power or control over those images, since he did not seem to have knowledge of the existence of browser cache. Conviction for possession was out of the question then, but this gap would have been filled perfectly

---

[151] See subsection 2.1.2.
[152] Stevens & Koops 2009.
[153] An acronym for the Dutch *Project motiveringsverbeteringen in strafvonnissen*; Project justification improvements in criminal judgments.
[154] See Nijboer 2011, p. 227–237.
[155] These judgments are, as chance would have it, specifically labelled as such (usually by the inclusion of the word PROMIS in its header), which makes finding them all the more easy. For this research, the database of www.rechtspraak.nl has been searched for “240b” and “promis” and this resulted in a collection of 50 judgments that have been analysed.
[156] Rb The Hague 26 November 2010, LJN BO5163.

by the criminalisation of access. Nevertheless, the court could not convict for accessing child pornography—unfortunately, the prosecution had only charged the suspect with *possession* of said images.[157]

4.3.3 Testimony of the suspect

It should, first and foremost, be noted that in the majority of cases in which the suspect is charged with possession of child pornography, he does not contest this charge and, in fact, often confesses to the crime. According to the interviewed investigators, almost all suspects are cooperative during the investigative phase and most confess. Of the 50 analysed PROMIS judgments, 29 suspects do not challenge (intent of) possession of (at least some of) the child pornography, though not all confess in so many words. This does not mean those other 21 all deny they possessed child pornography: these cases include judicial defences such as unlawfully obtained evidence,[158] unclear charges, or that none of the images can be considered child pornography.[159] All in all, only in a relatively small number of cases does the defence actually contest the possession or intent thereof.

Although a confession does not have the same status in Dutch criminal law as it does in for instance the US, such an affirmative statement of the suspect, coupled with an investigative report, is enough for a judicial conviction in the system of 338–344 DCCP.

4.3.4 Written records

Written records come in five flavours, listed in article 344, section 1 DCCP, although the fifth category encompasses 'every other written record', making every written document suited for being used for evidentiary foundations, as long as it can be read out aloud at trial.[160,161]

Of those, the second (investigative reports) and fourth (specialist[162] reports) categories are particularly relevant for child pornography cases. Although the fifth category (every other written record) is unlimited in scope, it seems to be rarely used

---

[157] Ultimately, the suspect in this case *was* convicted of possession of child pornography regarding images found on his home computer, which he burnt to a CD; a sufficient indication of power and control, according to the court.
[158] See, for instance, Rb Amsterdam 3 July 2009, LJN BJ8160.
[159] See, for instance, Rb Rotterdam 22 October 2009, LJN BK1007.
[160] Records need to be read out aloud, or at least summarised, at trial if they are to be admitted as evidence. See article 301 DCCP.
[161] Corstens 2008, p. 698 and Nijboer 2011, p. 203.
[162] The term 'specialist' is used here to denote what is known in Dutch as 'deskundige'. 'Expert' would be an equally good translation, were it not for the distinction Nijboer draws between specialists and experts: an expert has extensive knowledge in a specific field and his skill may be used in the investigation, but he does not become a specialist until specific conditions have been met. See for the distinction Nijboer 2009, p. 32. This thesis will follow that distinction.

in the cases, particularly since official investigative reports are preferable because of their added evidentiary value—section 2 of article 344 specifically states that a single investigative report is enough to base judicial conviction on. Nijboer calls this exception an undesirable course of action[163] and, fortunately, this option is rarely utilised in practice with respect to felonies. Nevertheless, most written records used for evidentiary foundation are investigative reports.

In Dutch criminal proceedings, quantitively, written records are the most important category of evidence,[164] and this is also true for investigations into digital child pornography. Of the five listed categories in article 344 DCCP, the investigative report of category two is present in virtually all analysed cases. At least one investigative report is included in each case file that describes, in detail, a random selection of five to ten of the child pornographic image and/or video files that were discovered in the suspect's possession, as explained in subparagraph 4.1.1. Investigative reports of suspect interrogations are another often found piece of evidence.

Under the correct circumstances, written records of specialist investigations can be used for evidentiary foundations. Specialist testimonies have their own category for when they are summoned to court to give their testimony there, but if they cannot or are not summoned, their findings (written down in a report) can still be used as evidentiary foundations through the use of this category. The next subsection will deal with specialist investigation in child pornography cases in detail.

As an elaborate example of the large number of written records involved in these types of cases, listed below are the records that were used as articles of evidence in the PROMIS case of Rb Groningen 12 April 2010[165]:

- An investigative report detailing the investigation of a BBS where child pornographic images were available for downloading, and from which those images were downloaded by a computer with an IP address that was part of the Hanzehogeschool.
- An investigative report explaining that analysis of those images showed that they were indeed child pornographic in nature.
- An investigative report stating that a computer was seized at the Hanzehogeschool, and that analysis of that computer turned up a sizable amount of child pornographic images.
- An investigative report of the analysis of the computer, showing that a certain user of the computer—that turned out to be the suspect—regularly downloaded such images.

---

[163] See Nijboer 2011, p. 77–78.
[164] Corstens 2008, p. 697.
[165] Rb Groningen 12 April 2010, LJN BM1069.

- An investigative report that explicitly details the video files that were found on the computer.
- An investigative report that explicitly details the image files that were found on the computer.
- A written record of a specialist in the area of forensic ICT investigation, explaining that a certain number images and video files were accessed twice by the computer user.

4.3.5 Testimony of a specialist[166]

A specialist is an expert in a particular field who has been appointed a specialist by any judge. Prior to 2010, judges had full discretion with regard to whom to appoint a specialist: the legislator left that question to the legal practice.[167] January 1st 2010, however, marked the introduction of the Experts in criminal cases act (*Wet deskundige in strafzaken*[168]), introducing with it the Dutch Register of Judicial Specialists (*Nederlands Register Gerechtelijk Deskundigen*[169]). This register maintains a list of specialists in several fields, with strict requirements for their quality and reliability.[170] There have been (and still are) such registers before, such as the National Register of Judicial Specialists (*Landelijk Register van Gerechtelijke Deskundigen*[171]), maintaining its own quality control for their experts, but these systems are *optional*, whereas the Dutch register aims to set obligatory requirements for all judicial specialists.[172] It is far from implemented completely, however. At the time of writing, only six categories with listed experts appear in the register—none of which include forensic expertise, let alone digital forensics. For those fields, the judicial discretion remains. Having said that, there might not an urgent need for digital forensic specialists in the Dutch register. As evident from the discussion on written records above and the interviews conducted for this thesis, much work in the digital field is done by investigative officers and investigative reports logging their work are just as good for evidence. This distinction will be discussed in more detail below.

Specialists in the criminal procedure can add what Nijboer calls something 'non-everyday': their particular education, practice and experience in a certain field allow them to add something to the investigation that others, with more general knowledge,

---

[166] In this subsection, both the summoning of a specialist and the usage of their reports by the judge as a written record are discussed. Although the latter is technically a written record, the procedure of appointing a specialist is the same for both.
[167] Nijboer 2011, p. 196.
[168] Wet van 22 januari 2009 tot wijziging van het Wetboek van Strafvordering tot verbetering van de regeling van de positie van de deskundige in het strafproces. See Nijboer 2009, p. 34 and p. 44.
[169] www.nrgd.nl.
[170] See also Nijboer 2011, p. 194.
[171] www.lrgd.nl.
[172] The newly added article 51k DCCP specifically states that specialists that are *not* listed in the register can only be appointed with sufficient justification.

cannot.[173] Nijboer differentiates the involvement of the specialist in three typical areas: education, counselling and investigation.[174]

In several of the analysed cases, judges employed specialists, either by directly summoning them or, more often, by using their reports. It seems most specialist usage involves work in the category of educating the judge, although the lines between the categories might be somewhat blurred in practice and, more importantly, it's hard to gather this knowledge from the available judgments. What follows is an accumulation of some examples of specialist usage in child pornography cases.

In the lower court of Amsterdam, a specialist was summoned to educate the judges on the intricacies of peer-to-peer software.[175] On the basis of that statement, the judges refuted the prosecutor's claim that it is a fact of common knowledge that peer-to-peer software automatically shares downloaded files with other interested parties. The specialist in the Groningen case of 12 April 2010 gave a statement on if and how often the computer user accessed certain files,[176] and the specialist in the Arnhem case of 26 October 2010 declared there had been a miscalculation of the number of child pornography files on the suspect's computer.[177] Finally, in a Maastricht case, the summoned specialist declared it very unlikely that large amounts of child pornography were downloaded automatically along with the files the suspect searched for.[178] Outside of the PROMIS cases, a specialist has been summoned in for instance Rb Zutphen 27 April 2011, declaring at the investigation at trial that it requires an act on the user's part to put files into folders the way they were located on the suspect's computer.[179]

All in all, though, it seems specialists are not often used regarding issues with digital evidence. Rather, in the analysed cases, most specialist usage involved psychologists giving statements on the suspect's sexual interests.[180] There might be a missed opportunity here for the judges, since specialists (especially after they are incorporated into the national register) might be so valuable for education and, more importantly perhaps, counselling.

Expert instruments cannot just be used by experts: 'ordinary' investigators can and often use those for the same purposes.[181] The Dutch Supreme Court admitted as much, affirming in 1993 that an investigative report can, under certain circumstances,

---

[173] Nijboer 2009, p. 38.
[174] Nijboer 2011, p. 195.
[175] Rb Amsterdam 3 July 2009, LJN BJ8160.
[176] Rb Groningen 12 April 2010, LJN BM1069.
[177] Rb Arnhem 26 October 2010, LJN BO1711.
[178] Rb Maastricht 26 May 2011, LJN BQ6221.
[179] Rb Zutphen 27 April 2011, LJN BQ2758.
[180] Many of the analysed cases involve suspects that are not only charged with possession of child pornography, but oftentimes also its production and abuse of children, in which case psychological research makes more sense.
[181] Nijboer 2009, p. 51.

be employed as a specialist report.[182] In 2009, the public prosecution department concerned itself with the matter and released an instruction,[183] explicitly detailing the difference between technical investigation and investigation conducted by specialists. In order to determine the difference between technical investigation and specialist investigation, the legislator hinged the distinction on the available areas of expertise within the police organisation. The distinction is important, not necessarily for the end result (both can be used as evidentiary foundation), but for the involvement of the defence in the investigation, the right to request contra-investigation etc. In section 4.5, the position of the suspect is examined in more detail.

As concluded in the previous chapter, specialist involvement is non-existent in the preparatory investigation: their involvement is not obligatory because of the non-destructiveness of the investigation, and the area of information technology is specifically assigned to investigative authorities, making it a matter of technical investigation. Regardless, it is evident from the overview above that specialists are still being summoned to the courtroom, not to assist investigators but the *judges* in their investigation, albeit in a relatively small number of cases. As Nijboer puts it[184]—and the interviewed investigators confirm this—a person that has conducted technical investigation during the preparatory investigation can, during the investigation at trial, still be summoned as a specialist.

4.3.6 Judge's own perception

Nijboer calls the category of the judge's own perception a 'rest category' compared to the other categories of evidence.[185] He provides several examples of evidence that can only be admitted in court by means of this category: displaying photographs or sketches or the playback of video footage, audio recordings or digital presentations.[186] Particularly the displaying of photographs is an important element of many cases involving child pornography. The perception should be personal, performed at trial (not based on something the judge heard somewhere) and it should be an objective perception, not a judgment (based on the senses, not on evaluation).[187]

Judicial perception is used as evidentiary foundation in innumerable cases where the suspect denies intent on possession because he was unaware either that the victims in his images were younger than 18 or that the images were sexual in nature. Courts often appear to decide on this by means of their own perception: the victim is

---

[182] HR 8 June 1993, *DD* 93.465. See also Nijboer 2011, p. 207.
[183] See footnote 106 in subsection 3.5.2.
[184] Nijboer 2011, p. 199.
[185] Albeit in a different sense from the 'rest category' of article 344, section 1. See Nijboer 2011, p. 176.
[186] Nijboer 2011, p. 177–180.
[187] Corstens 2008, p. 669.

obviously below 18 or the images are obviously sexually explicit—the specifics of which are beyond the scope of this thesis.

A single curious judicial perception in child pornography cases took place in 2006 in Breda.[188] The suspect denied intent on possession of child pornography images and claimed the images that were found on his computer did not involve the alleged victim, because he believed they had been altered. The court waived that defence, remarking—based on the court's own perception, which was backed up by the administrator of the National Database Child Pornography—that these images showed no signs of alteration, and claimed that in the case of photographs, the court can consider the reliability of the evidence by itself. Although formally 'just' a perception, it seems the court is close to actually *judging* the evidence in this particular example.

4.3.7 Facts of common knowledge

Facts of common knowledge are considered to be true and do not require evidential foundation unless challenged by the defence. Several technical issues have come up in recent years in the courtroom, with regard to what in the digital world is common knowledge and what is not. With regard to digital evidence in general, the following designations deserve to be mentioned.

As explained in subparagraph 4.2.4, time and place determine which facts can be considered common knowledge.[189] The lower court in Utrecht in particular has maintained that the fact that most browsers keep a cache and history of visited web pages is not *yet* a fact of common knowledge.[190] The courts in Zwolle and Middelburg, however, deem it to be common knowledge that files residing in the browser cache can easily be accessed by the average computer user and those files can be opened without complicated procedures.[191]

In the case of Rb 's-Hertogenbosch 17 December 2009, the court concluded that it is common knowledge that downloaded files are saved to the computer, if even in a temporary folder. This fact was deemed enough to have a reasonable suspicion arise against the suspect.

Curiously enough, the court in Almelo does consider common knowledge the fact that deleted files remain on the hard drive even after the recycling bin or trash is subsequently emptied.[192] The court concludes that this method will thus not permanently delete a file. Although it is certainly debatable whether or not this

---

[188] Rb Breda 4 August 2006, LJN AY5686.
[189] Nijboer 2011, p. 85.
[190] Rb Utrecht 31 May 2010, LJN BM9249, 24 September 2010, LJN BO1677, 7 October 2010, LJN BO2816.
[191] Rb Zwolle 28 October 2009, LJN BK7258 and Rb Middelburg 3 November 2010, LJN BO2782.
[192] Rb Almelo 3 August 2010, LJN BN3874.

information is common knowledge, the court seems to overlook the fact that in that reasoning, it is practically impossible for any computer user to permanently delete a file. The court in The Hague seems to be more realistic in stating that files residing in the unallocated clusters of a hard drive cannot be used without specialist software.[193]

In Amsterdam, the court denied common knowledge to the fact that peer-to-peer software by default is set up to automatically share all downloaded files with other interested parties.[194] The suspect in that case was cleared of charges of spreading child pornography.

In the Rb Leeuwarden case of 30 October 2008,[195] the suspect stated that the child pornography that was found on his cellular phone was placed there by the same computer virus that downloaded the images in the first place. The court debunked this with the following statement: it is a fact of common knowledge that a computer does not recognise a cellular phone as a memory to which files can be written.

Of particular importance, especially with respect to possible jurisdictional issues that may arise from trans-border cybercrime, is the court of Arnhem's designation of common knowledge to the fact that users from all over the world are active on the Internet and, more importantly, the fact that a particular user speaks a certain language does not necessarily mean that that user is located in a country where that language is spoken.[196] The suspect in this case was convicted for exporting child pornography. His rationalisation that the receiving party spoke Dutch—and was therefore likely to be located in the Netherlands—was rejected for that very reason.

The court in Zwolle deemed it a fact of common knowledge that spam email messages are delivered unwanted and often remain unread.[197] For this reason, it cannot be assumed the suspect in that case had intent on possession of the images of child pornography that were sent to him via email that ended up in his spam folder.

The advocate-general in the Dutch Supreme Court case of 30 September 2008 designated it to be a fact of common knowledge that files with the extension .avi are multimedia files. The suspect's defence—he had not known those files were video files, let alone child pornographic in nature—failed. The same advocate-general designated it a fact of common knowledge that Temporary Internet Files that are cached by the Internet Explorer browser have the extension .temp. This is, however, incongruous with the above-mentioned fact of common knowledge that websites are cached in the first place.

---

[193] Rb The Hague 26 November 2010, LJN BO5163 and 6 January 2011, LJN BP1920.
[194] Rb Amsterdam 3 July 2009, LJN BJ8160.
[195] Rb Leeuwarden 30 October 2008, LJN BG3632.
[196] Rb Arnhem 15 March 2010, LJN BL7418.
[197] Rb Zwolle 23 June 2010, LJN BM9613.

The court in Utrecht many times designated it to be a fact of common knowledge that individuals who view and download child pornography are prone to continue with that activity and usually keep hold of those images.[198]

4.4 Digital evidence difficulties

4.4.1 Authenticity and the chain of custody

Proving that a digital document of evidence is authentic comes down to proving that it has not been "modified, replaced or corrupted."[199] According to Mason, there are two aspects to this: the data should be subject to a chain of custody and the data should not be modified from the time it is collected, at least not without authority. Only by adhering to those two rules can the material be considered authentic when it is used as evidence in court.

As far as modification is concerned, Dutch digital investigation seems to be right on course. As explained above, data carriers are handled carefully, write-protected and investigation is exclusively carried out on the copy while the original carrier is safely stored away. Multiple tools are used to make multiple copies and, finally, a checksum process ensures the integrity of the copy. Maintaining a chain of custody is more problematic, however. When implemented correctly, a chain of custody is a (digital) record that chronologically lists all places the evidence has been and has been analysed or handled. If there is a gap in that list, the evidence has thus been somewhere unknown and this severely impacts its authenticity and reliability. According to the interviewed investigators, the system that is in place for keeping track of evidence is cumbersome in use and therefore not utilised consistently, defeating the whole purpose of the chain of custody. In fact, one investigator admitted in so many words that in the future, inevitably, a defendant will challenge the chain of custody of the incriminating evidence and investigators will not have an answer ready.

4.4.2 Understanding of legal professionals

The legislator does not expect judges to be knowledgeable in every single scientific field: for that, expert investigators and specialists can provide assistance. The increasing complexity of especially the technical field has required judges to rely more and more on these experts, requiring those judges to decide on the results of complex technical forensic investigation. Nijboer questions the ability of legal

---

[198] Rb Utrecht 12 May 2010, LJN BM5279, repeated by the same court on the same date in LJN BM5294 and LJN BN1466, and later in Rb Utrecht 21 May 2010, LJN BM8000 and Rb Utrecht 17 June 2010, LJN BM9229.
[199] Mason 2007, p. 84.

professionals to appreciate these results.[200] Lack of understanding of jargon is an important factor in this.[201] Van Koppen, in a critical overview of judicial decision-making, expressed that the decision regarding the evidence and guilt of the suspect is a factual decision, not a judicial one.[202] Because judges are legally educated, they inevitably have to decide on subjects they are not necessarily schooled in. Van Koppen proposes a scientific method to regulate this decision: judges should always be comparing scenarios: one that the charges describe and one or more others, in which the suspect is not guilty, and then logically falsify each alternative until one remains. He considers each possible scenario of events of the crime as a separate scientific theory that can never be proven, but when every likely alternative is falsified, the scenario that remains is at least most likely what really occurred.[203]

4.4.3 The judges and digital experts relationship

Nijboer, in a short historic overview, concludes that practitioners of law have always regarded forensic experts somewhat sceptically, given the tendency of the latter of pretentiousness in explaining the nature, degree and causes of crime.[204] In short, experts seem to have the propensity to *interpret* their findings, which is, in Dutch criminal procedure at least, the exclusive responsibility of the criminal judge: article 51i DCCP specifically states that specialists (only) provide information or conduct research. However, these specialists would have a hard time *not* interpreting certain facts, since by their very nature, many sciences have their own 'version' of the truth, one that is not necessarily in conformity with the criminal-judicial truth.[205] Still, the increasing complexity of society in recent decennia has made it a necessity for judicial decision-making to be supported by some form of expert counselling.

4.4.4 Standardisation

As explained above, there is no one standard procedure for conducting digital investigation. Many procedural documents have been written, particularly in the United States, but the radical diversity in digital investigations makes adopting a uniform plan of action difficult, if not impossible. This lack of standardisation has implications, however.

As Carney and Rogers pointed out in 2004, lack of standardisation brings with it the practical hindrance for investigators of needing to spell out time and time again both the specific course of action that they took in this particular investigation and the

---

[200] Nijboer 2011, p. 202.
[201] Nijboer 2009, p. 64. See for a practical example L. Essers, 'OM mist inzicht in encryptie Robert M.', Webwereld January 5, 2011, webwereld.nl/nieuws/105280/om-mist-inzicht-in-encryptie-robert-m-.html.
[202] Van Koppen 2011, p. 16.
[203] Van Koppen 2011, p. 73–76.
[204] Nijboer 2009, p. 22.
[205] Nijboer 2009, p. 37.

general concepts of digital investigation such as deleted files and timestamps—concepts that the recipients of those clarifications are rarely familiar with.[206] Standardisation might provide judges with more insight into the—often-incomprehensible—procedure of forensics in general and digital forensics in particular.

In contrast, Nijboer points out that standardisation might harm the defence's ability to object to the use of the evidence and jeopardises the judge's responsibility for completeness of the investigation, because the results of standardised investigations are held in such high regard in judicial practice.[207]

Carney and Rogers compare digital forensics to DNA and drug testing and come to the conclusion that both are particularly complicated to the uninitiated, yet the latter are perfectly accepted in court since the process has been standardized and is peer-reviewed. Nijboer advises the court to examine to what degree the results of the investigation are based on certain tests, methods and techniques.[208] It is practically impossible for them to check the concrete results of the investigation, but by employing the peer review system that most fields have, the judge can decide on the reliability of the evidence.

4.5 The defence

4.5.1 Rights of the suspect

The right to silence, a fundamental cornerstone of most criminal law systems, has been laid down in article 29 DCCP. Despite this right, the majority of suspects, particularly in child pornography cases, fully cooperate and provide answers to all questions of investigators, even going so far as providing passwords to incriminating and encrypted portions of their hard disks.

The results of the preparatory investigation are required to be included in detail, through investigative reports, in the case file.[209] The principle of right to equal information and, more practically, article 30 DCCP dictate that the defence should have access to that case file. However, what exactly goes into this file is not defined in either criminal code. The Dutch Supreme Court, in a 2001 case,[210] concluded that a hard drive is not part of the case file and, thus, that the suspect does not necessarily have to have access to the drive. The case file, according to the court, collects inculpatory and exculpatory evidence—a hard drive is neither, evidentially. In

---

[206] Carney & Rogers 2004, p. 2.
[207] For instance, the result of a blood test or a positive DNA match—two prominent examples of standardised investigations—are hardly open to objection.
[208] Nijboer 2011, p. 202.
[209] See Corstens 2008, chapter 9.3.
[210] HR 8 May 2001, LJN AB1517.

this particular case, the suspect was not put in a more unfavourable position by being denied access to the hard drive: a specialist was available for questioning, the suspect was not able to indicate any flaws in the investigation, and the he did not ask for a copy of the disk.

In recent years, the potential for the defence to conduct a contra-investigation has come to fruition. Judges routinely followed specialist conclusions, and only in the last decade did the inadequacies of specialist investigation receive attention.[211] The long-established article 263 DCCP has bestowed upon the defence the power to summon specialists at trial. In 2009, the Experts in criminal cases act[212] introduced several more means for the defence to influence the specialist investigation or, indeed, conduct an investigation of its own. These include the following.

The suspect can now make requests to the prosecutor or the judge-commissioner (depending on the stage of the preparatory investigation) to appoint a specialist (articles 150 and 227, section 1 DCCP, respectively). In the latter case, the suspect can even recommend a specific specialist—a recommendation that the judge-commissioner is obliged to follow (article 227, section 2). In all cases, the suspect can request that the specialist carry out certain additional investigation (articles 150a, section 1, 228, section 3 and 231, section 1). Most importantly, the suspect can make a request for contra-investigation, initially to the prosecutor (article 150a, section 3) but later—should the prosecutor refuse the request—to the judge-commissioner as well (article 150b, section 2).

It is important to note that the above-mentioned potential for specialist contra-expertise formally only exists when a specialist has already been involved in the case. As explained above, this is rarely the case in digital forensic investigation: this field is considered to be technical investigation of which the police force itself is more than capable of handling. Nevertheless, the power to summon a specialist at the investigation at trial still exists. Furthermore, the interviewed digital expertise investigators specifically mentioned that the defence is always welcome to make use of their facilities to conduct an investigation of their own, either by the defence attorney or a paid professional. There do, however, seem to exist some discrepancies with regard to whether or not a copy of the hard disk is allowed to leave the facility to be investigated elsewhere.

4.5.2 Defence catalogue

It is interesting to see that, although the virus or Trojan defence is mentioned countless times in the literature on the subject, and both interviewed investigators acknowledge that many suspects claim the virus ‘did it’, the defences are rarely found in court judgments: searching through the catalogue of some 500 cases

---

[211] Nijboer 2011, p. 200.
[212] See subsection 4.3.5.

involving article 240b DCCP, there is no relevant mention of 'Trojan'[213] and only a single instance of 'virus'. In the latter case,[214] the suspect indeed claimed a virus had both downloaded the child pornography and subsequently transferred those images to his cell phone. An important observation here is that the court did not reject the virus defence in so many words—it only refuted the claim that viruses can transfer data to cell phones autonomously. Nevertheless, the suspect was convicted for possession of child pornography because he seemed to have sufficient understanding of computers and did not make enough of an effort to get rid of the images. With that judgment, the court in Leeuwarden seems to accept that viruses might download illegal images without the user's consent; it is then up to the user to do everything in his power to remove those images permanently.

The I-was-hacked-defence makes an important appearance in a The Hague case of 2006.[215] Here, the suspect claims a hacker had infiltrated his computer and placed not only child pornography on it, but also traces of activity that linked the computer user to the child pornography and a privacy application—in essence, the suspect was framed. Specialist investigation conducted by the Netherlands Forensic Institute could neither confirm nor deny this statement. Compelled to decide, the court convicted the suspect. There were no contradictions found to the objection, but also no indications that it was true. Furthermore, the password to the privacy application consisted of a combination of the suspect's cigarette brand and his age, something that a hacker would not have known. The suspect claimed a keylog program had monitored his keystrokes and sent his passwords to the hacker this way, but the court was not convinced a hacker would go through such great lengths to frame the suspect. Furthermore, the keylog logs specifically showed extensive activity with regard to pornography.

Some other interesting defences regarding digital evidence have been raised as well. In several cases, the suspect claimed it was not he who put child pornography on the computer, but someone else who had access to it. Often, the court does not consider this defence plausible and rejects it.[216] Only in one case did the court accept the excuse.[217] The suspect claimed it might have been friends of his who put the illegal material on his computer, and the court—while acknowledging this account to be highly unlikely—was not convinced beyond reasonable doubt that the suspect had intent on possession.

---

[213] Searching for '240b' and 'Trojan' returns only a single result, in which the suspect was accused of hacking in addition to possession of child pornography—he allegedly used a Trojan for the first offence.
[214] Rb Leeuwarden 30 October 2008, LJN BG3632. Also see subsection 4.3.7.
[215] Rb The Hague 31 July 2006, LJN AY5348.
[216] Rb Arnhem 3 August 2010, LJN BN3053 and 26 October 2010, LJN BO1711.
[217] Rb Zutphen 18 November 2009, LJN BK3748.

A few suspects deny possession because they had deleted the images and the files were only found in unallocated clusters on the hard drive. A suspect in Arnhem[218] was nevertheless convicted for possession because other evidence proves that the files were on his computer for at least a while with him knowing about it: he specifically requested child pornography from the other party of a chat conversation. The court in Maastricht[219] also rejected the excuse: the suspect typically checked what was downloaded and these files have remained accessible on his computer for at least a few months.

In one case, earlier mentioned in paragraph 4.3.7, the suspect claimed a virus was at work, specifically one that downloaded the child pornography to his cell phone. The court stated that, based on other evidence, the suspect appeared to be well aware of the child pornography in his possession and thus rejected the defence.

A defence that is often heard is the fact that the child pornography is an unwanted bycatch of other (legal) pornography. This defence was raised in seven PROMIS cases but accepted in none. Suspects were proven to have at least conditional intent[220] on possession,[221] continued their practice of downloading large amounts of pornography after discovering some illegal material was included,[222] or were not believed because their illegal files were neatly sorted into respective folders—something that requires an operative action on the user's side, according to the investigator.[223] A last example involved a suspect actively searching for "teens" in his Internet activity, according to evidence logs—he, too, was convicted.[224]

Another often-heard defence is that the child pornography was already on the data carrier when the suspect acquired it second-hand, and this defence is never accepted as well—in all three cases because of contradictory statements of the suspect regarding the nature and origin of the data carriers.[225]

Finally, an interesting defence was raised in an Arnhem case.[226] The suspect claimed the application Ghost Image kept automatically recovering the deleted images. The court rejected that claim with the fact that the child pornography files were, once again, neatly sorted in folders.

---

[218] Rb Arnhem 15 March 2010, LJN BL7418.
[219] Rb Maastricht 26 May 2011, LJN BQ6221.
[220] Conditional intent is enough for conviction of possession of child pornography. See Stevens & Koops 2009.
[221] Rb 's-Hertogenbosch 29 October 2008, LJN BG3640.
[222] Rb Groningen 12 April 2010, LJN BM1069.
[223] Rb Arnhem 26 October 2010, LJN BO1711.
[224] Rb Arnhem 3 August 2010, LJN BN3053.
[225] Rb Haarlem 16 March 2010, LJN BL9118, Rb Almelo 3 August 2010, LJN BN3874 and Rb Maastricht 26 May 2011, BQ6221.
[226] Rb Arnhem 26 October 2010, LJN BO1711.

4.5.3 Defence strategy

The above-mentioned defences challenge particular evidence in order to prevent the judge's conviction, resulting in the suspect's acquittal. Nijboer discerns four situations that result in the suspect's acquittal: (1) there are an insufficient number of statutory means of evidence; (2) the judge considers certain evidence to be obtained unlawfully and sets it aside, leaving insufficient evidence for conviction; (3) the judge considers certain evidence to be unreliable and sets it aside, once again leaving insufficient evidence for conviction; and (4) despite adequate means of evidence, the judge is not convinced of the suspect's guilt.[227] Of these, the first is well beyond the defence's control, but the other three situations can be influenced with strategic defences. Pijnen and Fennell-van Esch state regarding digital evidence, "the main role of the defence is to question whether the evidence collected (…) is trustworthy and convincing."[228] Adding Nijboer's second acquittal situation to that, this signifies the defence to focus on unreliable, unconvincing and unlawfully obtained evidence. Note that circumstances that would lead to an acquittal have to become *plausible*, and do not necessarily have to be proven to be true.[229]

Objections to the reliability of the evidence might for instance relate to the method of digital investigation, the way digital evidence is handled or, perhaps most importantly, the chain of custody of the evidence. Traditionally, two classic Dutch Supreme Court cases are mentioned with regard to unreliable evidence: the 'poppenspel'[230] and 'schoenmaker'[231] judgments jointly oblige judges to specifically state reasons for refuting substantiated objections of unreliability against evidence. [232] Their value today is uncertain, since judges are now obliged to do the same with any explicitly substantiated statements.[233]

Ferraro and Casey mention the creation of confusion as way to create reasonable doubt, thereby influencing judicial conviction.[234] However, the authors refer to the American common law system, where juries are known to be easily influenced and confused. Judges are inherently more even-handed, and spreading confusion does not seem to affect their judgment. In one case, mentioned in the previous subparagraph,[235] the suspect successfully presented the (unlikely) possibility that one of his friends planted child pornography on his computer. Such objection, in which an alternate—plausible—explanation of events does not conflict with any evidence[236]

---

[227] Nijboer 2011, p. 250.
[228] Pijnen & Fennell-van Esch in: Mason 2008, p. 625.
[229] Nijboer 2011, p. 75.
[230] HR 28 February 1989, *NJ* 1989, 748.
[231] HR 27 January 1998, *NJ* 1998, 404.
[232] Broeders 2003, p. 73.
[233] See subsection 4.2.3.
[234] Ferraro & Casey 2005, p. 278.
[235] Rb Arnhem 15 March 2010, LJN BL7418.
[236] Nijboer 2011, p. 136.

(known in Dutch legal theory as 'Meer en Vaart' objections, after the famous 1972 judgment[237]), appears to be a compelling option for defence strategy. At the very least, they require a substantiated refusal, and they force investigators (in subsequent cases) to investigative to a higher degree of impermeability. In this particular case, digital user logs, application usage logs or even circumstantial evidence found around the computer might have shown who was using a computer at a particular time. If, with additional evidence, there is still a plausible alternate explanation of events possible, the existing reasonable doubt would prevent a conviction. However, the hacker case in The Hague[238] has shown that courts will not be easily convinced of an alternate explanation, even when backed up by plenty of digital evidence.

[237] HR 1 February 1972, *NJ* 1974, 450.
[238] Rb The Hague 31 July 2006, LJN AY5348.

5 CONCLUSION

5.1 Reflection

5.1.1 Investigating digital evidence

Although Dutch forensic procedure is not regulated in guidelines, it is remarkably streamlined. Evidence is correctly handled and stored and given the specialist attention it deserves. Investigators are well educated in digital forensics and keep up-to-date with new developments in both hardware and software. They use state-of-the-art forensic software and know how to use it. Although there has, as of yet, been no specific training for dealing with investigations into accessing child pornography, investigators already include browser cache and history and other signs that link the user to child pornography in their investigation. Remarkably, the procedures are even streamlined between the different teams across the country, by virtue of intensive intercommunication. In that regard, investigators rightly so state that written regulation is unnecessary. However, the numerous guides from for instance the U.S. Department of Justice and the British Association of Chief Police Officers prove that written regulation is very well possible. In fact, Dutch procedure practice mostly matches up with the recommendations outlined in those documents as it stands.

The fact that the investigative process is not documented might be very problematic with regard to the chain of custody. Right now, a clever defence attorney might challenge that chain when the opportunity arises, and investigators might not have an answer ready. Strict guidelines with regard to evidence handling and responsibility would make certain that investigators always know where the evidence is and where it has been. It should be noted again that current procedures work suitably in practice, but the possibility of a gap in the chain of custody is a risk of sufficient importance to justify another attempt at drafting guidelines.

There are more difficulties with digital forensic procedure—not with its Dutch implementation, but with the science in general and the fact that investigators are bound by the framework of legislation within which they have to operate. Activity on the 'hidden' Internet (newsgroups and Usenet, BBS) is still very hard, if not impossible, to trace. There is still a problem with remote storage, particularly when the remote storage location is international or, even more problematic, when it is unknown: suspects may have uploaded their child pornography files to a remote file server that cannot or *may* not be accessed by investigators, thereby deadlocking the investigation. Encryption is another thorn in the investigation's side. When used with a key of considerable size (256-bit and upwards), investigators lack the computing power to crack encryption brute-force, and if the decryption key is not otherwise available and there are no non-encrypted child pornography files present, the

investigation will once more come to a dead end. Then again, the period of prescription for crimes relating to child pornography is twelve years.[239] Moore's Law[240] states that the amount of transistors on a computer processor—and thus its processing power—roughly doubles every two years. An encryption too elaborate to break brute-force by investigators today might be cracked in a more practical timespan in 12 years, when processors are 64 times as fast.

Many suspects are willing to work with investigators and many suspects, although trying to conceal their criminal activity, leave an opening in their protection. However, if a technologically savvy child pornographer wants his collection to be hidden and is willing to go to great lengths to keep it that way, between such mentioned technologies as remote storage and encryption, digital investigation will turn up nothing.

As far as investigating access to child pornography goes, there seem to be few possible evidentiary leads for the offence: either there are also images in possession of the suspect, or there are no traces of child pornography at all on the computer. ISPs might be in the best position to assist in finding evidence for accessing child pornography. Every Internet use requires an ISP, even at a public library or café, and those might have their own way of confirming who used the connection at what time. Still, by employing such effective technologies as network proxies, even accessing child pornography can be successfully hidden—if criminals are willing to make the technological investment.

5.1.2 Digital evidence in court

Dutch courts are no strangers to digital evidence but do seem to have some difficulty adapting to new technologies. Fortunately, the vast majority of child pornography cases are clear-cut and need little more evidence than an investigative report stating that child pornography was found on the suspect's computer. As long as the defence does not contest any of this evidence, judges are perfectly fine with accepting the digital investigation results as evidence.

There have, however, been a handful of cases in which judicial dealings with technical matters seem somewhat unusual. There seem to be quite some discrepancies between the courts of what is to be considered common knowledge with regard to Internet browser cache: the Utrecht court has consistently maintained throughout 2010 that the fact that web browsers maintain a cache of all visited pages is *not* (yet) common knowledge, whereas the courts in Middelburg and Zwolle consider it to be common knowledge that browser cache can be accessed by average computer users, implying that the mere existence of browser cache is

---

[239] Article 70, section 1 DCC.
[240] As predicted by Intel co-founder Gordon Moore in 1965, and still valid to this day. See download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_2pg.pdf.

common knowledge as well. The Almelo case in which the court concluded that deleting a file and subsequently emptying the recycling bin does not permanently erase a file is another curious example since, as said above, there is no way for average and even above-average computer users to get rid of files that way.

Aside from those few oddities, judges seem to rely mostly on digital investigators and their work, thereby giving most interpretative work out of hand. Legal professional are not and cannot be knowledgeable on all technical matters, but society nevertheless insists on judges to decide on them. A specialist to counsel the court on technical matters would fill this void perfectly, but they are rarely summoned to court, unfortunately. Perhaps judges are not (yet) used to the possibility of summoning a digital specialist, unlike their readiness to summon a behavioural expert.

5.2 Future considerations

Digital investigators are staying up to date with technological changes. They experiment with new digital hardware and software to learn the evidential implications of those products first-hand and regularly upgrade their systems and investigative software to the latest developments. Legal professionals, especially judges, are rarely technically educated, however. As discussed above, they nevertheless are expected to decide on technical questions of fact. An amusing anecdote of one of the interviewed investigators told the story of a judge who, acknowledging his own lack of understanding the subject, read through an “Internet for Dummies” book. When the investigator was summoned to court as a specialist, this judge showed the book and admitted that it was all the foreknowledge he possessed, prompting the investigator to explain from there.

This story marks two interesting points. One, judges seem to be ready to admit their own lack of technical understanding and—more importantly—willing to catch up on it, and two, investigators are sometimes summoned in court to aid in counselling and education for the judges. Unfortunately, specialists are too rarely involved in these cases, leading to judges making some of the curious technical findings described above. Perhaps a permanent digital specialist for judicial counselling, or even a specialised digital court,[241] might remedy the problem to an extent—the feasibility of which is beyond the scope of this thesis.

Lack of standardisation of the digital forensic procedure—not the lack of written procedure in the Netherlands, but rather a more general absence of one uniform procedure—hinders the acceptance of certain methods in court. Once again, DNA-

[241] The court in The Hague has a department of Intellectual Property, dealing exclusively with cases that involve IP-disputes. A similar department might be set up for cases involving (complicated) digital evidence.

fingerprinting is an equally complicated procedure to the uninitiated, but perfectly accepted as evidence because of its standardisation.

Several attempts have been made in the past to standardise at least certain aspects of digital forensics. The Common Digital Evidence Storage Format Working Group[242] was established in order to attempt to streamline the process of sharing digital evidence between different actors by creating a standard format. The working group was disbanded in 2007 because of lack of resources. Grobler has researched the state-of-the-art with regard to digital forensic standards and has found two standards the International Organization for Standardization (ISO) is currently working on: a standard for identification, acquisition and preservation of digital evidence in order to facilitate exchange of evidence between jurisdictions, and a standard for digital forensic governance. He concludes that jurisdictional incompatibilities in particular limit the development of international standards.[243] This is, of course, not to say that *national* standards cannot come to fruition.

[242] www.dfrws.org/CDESF/index.shtml.
[243] Grobler 2010.

6 BIBLIOGRAPHY

Britz 2009 M.T. Britz, *Computer forensics and cyber crime*, Upper Saddle River, NJ: Prentice Hall 2009.

Broeders 2003 A.P.A. Broeders, *Op zoek naar de bron: over de grondslagen van de criminalistiek en de waardering van het forensisch bewijs*, Deventer: Kluwer 2003.

Carney & Rogers 2004 M. Carney & M. Rogers, 'The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction', *International Journal of Digital Evidence* Spring 2004, Volume 2, Issue 4.

Casey 2004 E. Casey, *Digital Evidence and Computer Crime*, London: Academic Press 2004.

Chisum & Turvey 2000 W.J. Chisum & B. Turvey, 'Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction', *Journal of Behavioral Profiling*, January 2000, vol. 1, no. 1. Available online at www.profiling.org/journal/vol1_no1/jbp_ed_january2000_1-1.html.

Cleiren & Nijboer 2009 C.P.M. Cleiren, J.F. Nijboer, *Tekst & Commentaar, Strafvordering*, achtste druk, Deventer: Kluwer 2009.

Cohen & Galynker 2009 L.J. Cohen & I. Galynker, 'Psychopathology and Personality Traits of Pedophiles', *Psychiatric Times* 2009, Vol. 26, No. 6.

Corstens 2008 G.J.M. Corstens, *Het Nederlands Strafprocesrecht*, Deventer: Kluwer 2008.

Ferraro & Casey 2005 M.M. Ferraro & E. Casey, *Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science*, London: Academic Press 2005.

Grobler 2010 M.M. Grobler, *Digital forensic standards: international progress*, South African Information Security Multi-Conference (SAISMC), Port Elizabeth, South Africa, 17–18 May 2010, pp. 261–271.

Van Kampen 1998 P.T.C. van Kampen, *Expert Evidence Compared: Rules and practices in the Dutch and American Criminal Justice System*, Antwerpen—Groningen: Intersentia Rechtswetenschappen 1998.

Keulen et al. 2010 B.F. Keulen, H.K. Elzinga, N.J.M. Kwakman, J.A. Nijboer, *Het deskundigenregister in strafzaken: de beoogde werking, mogelijke neveneffecten en risico's*, Den Haag: Boom juridische uitgevers 2010.

Koops 2010 E.J. Koops, 'Cybercrime Legislation in the Netherlands', *Electronic Journal of Comparative Law* 2010, Volume 14.3.

Van Koppen 2011 P.J. van Koppen, *Overtuigend bewijs: indammen van rechterlijke dwalingen*, Amsterdam: Nieuw Amsterdam uitgevers, 2011.

KPMG 2004 KPMG Informatie Risk Management, 'Onderzoek naar de opslag van historische verkeersgegevens van telecommunicatieaanbieders', Amstelveen: KPMG 2004.

Mason 2007 S. Mason, *Electronic Evidence*, London: LexisNexis 2007.

Mason 2008 S. Mason, *International Electronic Evidence*, London: British Institute of International and Comparative Law 2008.

Nijboer 2009 J.F. Nijboer, *Forensische expertise*, Deventer: Kluwer 2009.

Nijboer 2011 J.F. Nijboer, *Strafrechtelijk Bewijsrecht*, Deventer: Kluwer 2011.

Oerlemens 2010 J.J. Oerlemans, *Opsporing en bestrijding van kinderpornografie op internet*, Tilburg: Celcus juridische uitgeverij 2010.

Ohm 2008 P. Ohm, 'The Rise and Fall of Invasive ISP Surveillance', *University of Illinois Law Review* 2009, p. 1417–1496.

Stevens & Koops 2009 L. Stevens & E.J. Koops, 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno', *Delikt en Delinkwent*, *39*(7), 669-696.

Wall 2007 D.S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity Press 2007.

Wortley & Smallbone 2006 R. Wortley & S. Smallbone, 'Child Pornography on the Internet', *Problem-Oriented Guides for Police–Problem-Specific Guide Series*, No. 41.