= Digital forensics =

Digital forensics ( sometimes known as digital forensic science ) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices , often in relation to computer crime . The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data . With roots in the personal computing revolution of the late 1970s and early 1980s , the discipline evolved in a haphazard manner during the 1990s , and it was not until the early 21st century that national policies emerged .

Digital forensics investigations have a variety of applications . The most common is to support or refute a hypothesis before criminal or civil ( as part of the electronic discovery process ) courts . Forensics may also feature in the private sector ; such as during internal corporate investigations or intrusion investigation ( a specialist probe into the nature and extent of an unauthorized network intrusion ) .

The technical aspect of an investigation is divided into several sub @-@ branches , relating to the type of digital devices involved ; computer forensics , network forensics , forensic data analysis and mobile device forensics . The typical forensic process encompasses the seizure , forensic imaging ( acquisition ) and analysis of digital media and the production of a report into collected evidence .

As well as identifying direct evidence of a crime , digital forensics can be used to attribute evidence to specific suspects , confirm alibis or statements , determine intent , identify sources ( for example , in copyright cases ) , or authenticate documents . Investigations are much broader in scope than other areas of forensic analysis ( where the usual aim is to provide answers to a series of simpler questions ) often involving complex time @-@ lines or hypotheses .

= = History = =

Prior to the 1980s crimes involving computers were dealt with using existing laws . The first computer crimes were recognized in the 1978 Florida Computer Crimes Act , which included legislation against the unauthorized modification or deletion of data on a computer system . Over the next few years the range of computer crimes being committed increased , and laws were passed to deal with issues of copyright , privacy / harassment ( e.g. , cyber bullying , cyber stalking , and online predators ) and child pornography . It was not until the 1980s that federal laws began to incorporate computer offences . Canada was the first country to pass legislation in 1983 . This was followed by the US Federal Computer Fraud and Abuse Act in 1986 , Australian amendments to their crimes acts in 1989 and the British Computer Misuse Act in 1990 .

= = = 1980s ? 1990s : Growth of the field = = =

The growth in computer crime during the 1980s and 1990s caused law enforcement agencies to begin establishing specialized groups , usually at the national level , to handle the technical aspects of investigations . For example , in 1984 the FBI launched a Computer Analysis and Response Team and the following year a computer crime department was set up within the British Metropolitan Police fraud squad . As well as being law enforcement professionals , many of the early members of these groups were also computer hobbyists and became responsible for the field 's initial research and direction .

One of the first practical ( or at least publicized ) examples of digital forensics was Cliff Stoll 's pursuit of hacker Markus Hess in 1986 . Stoll , whose investigation made use of computer and network forensic techniques , was not a specialized examiner . Many of the earliest forensic examinations followed the same profile .

Throughout the 1990s there was high demand for these new , and basic , investigative resources . The strain on central units lead to the creation of regional , and even local , level groups to help handle the load . For example , the British National Hi @-@ Tech Crime Unit was set up in 2001 to provide a national infrastructure for computer crime ; with personnel located both centrally in London

and with the various regional police forces ( the unit was folded into the Serious Organised Crime Agency ( SOCA ) in 2006 ) .

During this period the science of digital forensics grew from the ad @-@ hoc tools and techniques developed by these hobbyist practitioners . This is in contrast to other forensics disciplines which developed from work by the scientific community . It was not until 1992 that the term " computer forensics " was used in academic literature ( although prior to this it had been in informal use ) ; a paper by Collier and Spaul attempted to justify this new discipline to the forensic science world . This swift development resulted in a lack of standardization and training . In his 1995 book , " High @-@ Technology Crime : Investigating Cases Involving Computers " , K Rosenblatt wrote :

Seizing , preserving , and analyzing evidence stored on a computer is the greatest forensic challenge facing law enforcement in the 1990s . Although most forensic tests , such as fingerprinting and DNA testing , are performed by specially trained experts the task of collecting and analyzing computer evidence is often assigned to patrol officers and detectives .

= = = 2000s : Developing standards = = =

Since 2000 , in response to the need for standardization , various bodies and agencies have published guidelines for digital forensics . The Scientific Working Group on Digital Evidence ( SWGDE ) produced a 2002 paper , " Best practices for Computer Forensics " , this was followed , in 2005 , by the publication of an ISO standard ( ISO 17025 , General requirements for the competence of testing and calibration laboratories ) . A European lead international treaty , the Convention on Cybercrime , came into force in 2004 with the aim of reconciling national computer crime laws , investigative techniques and international co @-@ operation . The treaty has been signed by 43 nations ( including the US , Canada , Japan , South Africa , UK and other European nations ) and ratified by 16 .

The issue of training also received attention . Commercial companies ( often forensic software developers ) began to offer certification programs and digital forensic analysis was included as a topic at the UK specialist investigator training facility , Centrex .

Since the late 1990s mobile devices have become more widely available , advancing beyond simple communication devices , and have been found to be rich forms of information , even for crime not traditionally associated with digital forensics . Despite this , digital analysis of phones has lagged behind traditional computer media , largely due to problems over the proprietary nature of devices .

Focus has also shifted onto internet crime , particularly the risk of cyber warfare and cyberterrorism . A February 2010 report by the United States Joint Forces Command concluded :

Through cyberspace , enemies will target industry , academia , government , as well as the military in the air , land , maritime , and space domains . In much the same way that airpower transformed the battlefield of World War II , cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication .

The field of digital forensics still faces unresolved issues . A 2009 paper , " Digital Forensic Research : The Good , the Bad and the Unaddressed " , by Peterson and Shenoi identified a bias towards Windows operating systems in digital forensics research . In 2010 Simson Garfinkel identified issues facing digital investigations in the future , including the increasing size of digital media , the wide availability of encryption to consumers , a growing variety of operating systems and file formats , an increasing number of individuals owning multiple devices , and legal limitations on investigators . The paper also identified continued training issues , as well as the prohibitively high cost of entering the field .

= = = Development of forensic tools = = =

During the 1980s very few specialized digital forensic tools existed , and consequently investigators often performed live analysis on media , examining computers from within the operating system using existing sysadmin tools to extract evidence . This practice carried the risk of modifying data on

the disk , either inadvertently or otherwise , which led to claims of evidence tampering . A number of tools were created during the early 1990s to address the problem .

The need for such software was first recognized in 1989 at the Federal Law Enforcement Training Center , resulting in the creation of IMDUMP ( by Michael White ) and in 1990 , SafeBack ( developed by Sydex ) . Similar software was developed in other countries ; DIBS ( a hardware and software solution ) was released commercially in the UK in 1991 , and Rob McKemmish released Fixed Disk Image free to Australian law enforcement . These tools allowed examiners to create an exact copy of a piece of digital media to work on , leaving the original disk intact for verification . By the end of the 1990s , as demand for digital evidence grew more advanced commercial tools such as EnCase and FTK were developed , allowing analysts to examine copies of media without using any live forensics . More recently , a trend towards " live memory forensics " has grown resulting in the availability of tools such as WindowsSCOPE .

More recently the same progression of tool development has occurred for mobile devices ; initially investigators accessed data directly on the device , but soon specialist tools such as XRY or Radio Tactics Aceso appeared .

= = Forensic process = =

A digital forensic investigation commonly consists of 3 stages : acquisition or imaging of exhibits , analysis , and reporting . Ideally acquisition involves capturing an image of the computer 's volatile memory ( RAM ) and creating an exact sector level duplicate ( or " forensic duplicate " ) of the media , often using a write blocking device to prevent modification of the original . However , the growth in size of storage media and developments such as cloud computing have led to more use of ' live ' acquisitions whereby a ' logical ' copy of the data is acquired rather than a complete image of the physical storage device . Both acquired image ( or logical copy ) and original media / data are hashed ( using an algorithm such as SHA @-@ 1 or MD5 ) and the values compared to verify the copy is accurate .

During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools . In 2002 , an article in the International Journal of Digital Evidence referred to this step as " an in @-@ depth systematic search of evidence related to the suspected crime . " In 2006 , forensics researcher Brian Carrier described an " intuitive procedure " in which obvious evidence is first identified and then " exhaustive searches are conducted to start filling in the holes . "

The actual process of analysis can vary between investigations , but common methodologies include conducting keyword searches across the digital media ( within files as well as unallocated and slack space ) , recovering deleted files and extraction of registry information ( for example to list user accounts , or attached USB devices ) .

The evidence recovered is analysed to reconstruct events or actions and to reach conclusions , work that can often be performed by less specialised staff . When an investigation is complete the data is presented , usually in the form of a written report , in lay persons ' terms .

= = Application = =

Digital forensics is commonly used in both criminal law and private investigation . Traditionally it has been associated with criminal law , where evidence is collected to support or oppose a hypothesis before the courts . As with other areas of forensics this is often as part of a wider investigation spanning a number of disciplines . In some cases the collected evidence is used as a form of intelligence gathering , used for other purposes than court proceedings ( for example to locate , identify or halt other crimes ) . As a result , intelligence gathering is sometimes held to a less strict forensic standard .

In civil litigation or corporate matters digital forensics forms part of the electronic discovery ( or eDiscovery ) process . Forensic procedures are similar to those used in criminal investigations , often with different legal requirements and limitations . Outside of the courts digital forensics can

form a part of internal corporate investigations .

A common example might be following unauthorized network intrusion . A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise . Both to establish the extent of any intrusion and in an attempt to identify the attacker . Such attacks were commonly conducted over phone lines during the 1980s , but in the modern era are usually propagated over the Internet .

The main focus of digital forensics investigations is to recover objective evidence of a criminal activity ( termed actus reus in legal parlance ) . However , the diverse range of data held in digital devices can help with other areas of inquiry .

Attribution

Meta data and other logs can be used to attribute actions to an individual . For example , personal documents on a computer drive might identify its owner .

Alibis and statements

Information provided by those involved can be cross checked with digital evidence . For example , during the investigation into the Soham murders the offender 's alibi was disproved when mobile phone records of the person he claimed to be with showed she was out of town at the time .

Intent

As well as finding objective evidence of a crime being committed , investigations can also be used to prove the intent ( known by the legal term mens rea ) . For example , the Internet history of convicted killer Neil Entwistle included references to a site discussing How to kill people .

Evaluation of source

File artifacts and meta @-@ data can be used to identify the origin of a particular piece of data ; for example , older versions of Microsoft Word embedded a Global Unique Identifer into files which identified the computer it had been created on . Proving whether a file was produced on the digital device being examined or obtained from elsewhere ( e.g. , the Internet ) can be very important .

Document authentication

Related to " Evaluation of source , " meta data associated with digital documents can be easily modified ( for example , by changing the computer clock you can affect the creation date of a file ) . Document authentication relates to detecting and identifying falsification of such details .

= = = Limitations = = =

One major limitation to a forensic investigation is the use of encryption ; this disrupts initial examination where pertinent evidence might be located using keywords . Laws to compel individuals to disclose encryption keys are still relatively new and controversial .

= = Legal considerations = =

The examination of digital media is covered by national and international legislation . For civil investigations , in particular , laws may restrict the abilities of analysts to undertake examinations . Restrictions against network monitoring , or reading of personal communications often exist . During criminal investigation , national laws restrict how much information can be seized . For example , in the United Kingdom seizure of evidence by law enforcement is governed by the PACE act . During its existence early in the field , the " International Organization on Computer Evidence " ( IOCE ) was one agency that worked to establish compatible international standards for the seizure of evidence .

In the UK the same laws covering computer crime can also affect forensic investigators . The 1990 computer misuse act legislates against unauthorised access to computer material ; this is a particular concern for civil investigators who have more limitations than law enforcement .

An individuals right to privacy is one area of digital forensics which is still largely undecided by courts . The US Electronic Communications Privacy Act places limitations on the ability of law enforcement or civil investigators to intercept and access evidence . The act makes a distinction between stored communication ( e.g. email archives ) and transmitted communication ( such as

VOIP ) . The latter , being considered more of a privacy invasion , is harder to obtain a warrant for . The ECPA also affects the ability of companies to investigate the computers and communications of their employees , an aspect that is still under debate as to the extent to which a company can perform such monitoring .

Article 5 of the European Convention on Human Rights asserts similar privacy limitations to the ECPA and limits the processing and sharing of personal data both within the EU and with external countries . The ability of UK law enforcement to conduct digital forensics investigations is legislated by the Regulation of Investigatory Powers Act .

= = = Digital evidence = = =

When used in a court of law digital evidence falls under the same legal guidelines as other forms of evidence ; courts do not usually require more stringent guidelines . In the United States the Federal Rules of Evidence are used to evaluate the admissibility of digital evidence , the United Kingdom PACE and Civil Evidence acts have similar guidelines and many other countries have their own laws . US federal laws restrict seizures to items with only obvious evidential value . This is acknowledged as not always being possible to establish with digital media prior to an examination .

Laws dealing with digital evidence are concerned with two issues : integrity and authenticity . Integrity is ensuring that the act of seizing and acquiring digital media does not modify the evidence ( either the original or the copy ) . Authenticity refers to the ability to confirm the integrity of information ; for example that the imaged media matches the original evidence . The ease with which digital media can be modified means that documenting the chain of custody from the crime scene , through analysis and , ultimately , to the court , ( a form of audit trail ) is important to establish the authenticity of evidence .

Attorneys have argued that because digital evidence can theoretically be altered it undermines the reliability of the evidence . US judges are beginning to reject this theory , in the case US v. Bonallo the court ruled that " the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness . " In the United Kingdom guidelines such as those issued by ACPO are followed to help document the authenticity and integrity of evidence .

Digital investigators , particularly in criminal investigations , have to ensure that conclusions are based upon factual evidence and their own expert knowledge . In the US , for example , Federal Rules of Evidence state that a qualified expert may testify ? in the form of an opinion or otherwise ? so long as :

( 1 ) the testimony is based upon sufficient facts or data , ( 2 ) the testimony is the product of reliable principles and methods , and ( 3 ) the witness has applied the principles and methods reliably to the facts of the case .

The sub @-@ branches of digital forensics may each have their own specific guidelines for the conduct of investigations and the handling of evidence . For example , mobile phones may be required to be placed in a Faraday shield during seizure or acquisition to prevent further radio traffic to the device . In the UK forensic examination of computers in criminal matters is subject to ACPO guidelines . There are also international approaches to providing guidance on how to handle electronic evidence . The " Electronic Evidence Guide " by the Council of Europe offers a framework for law enforcement and judicial authorities in countries who seek to set up or enhance their own guidelines for the identification and handling of electronic evidence .

= = = Investigative tools = = =

The admissibility of digital evidence relies on the tools used to extract it . In the US , forensic tools are subjected to the Daubert standard , where the judge is responsible for ensuring that the processes and software used were acceptable . In a 2003 paper Brian Carrier argued that the Daubert guidelines required the code of forensic tools to be published and peer reviewed . He concluded that " open source tools may more clearly and comprehensively meet the guideline requirements than would closed source tools . "

= = Branches = =

Digital forensics includes several sub @-@ branches relating to the investigation of various types of devices , media or artifacts .

= = = Computer forensics = = =

The goal of computer forensics is to explain the current state of a digital artifact ; such as a computer system , storage medium or electronic document . The discipline usually covers computers , embedded systems ( digital devices with rudimentary computing power and onboard memory ) and static memory ( such as USB pen drives ) .

Computer forensics can deal with a broad range of information ; from logs ( such as internet history ) through to the actual files on the drive . In 2007 prosecutors used a spreadsheet recovered from the computer of Joseph E. Duncan III to show premeditation and secure the death penalty . Sharon Lopatka 's killer was identified in 2006 after email messages from him detailing torture and death fantasies were found on her computer .

= = = Mobile device forensics = = =

Mobile device forensics is a sub @-@ branch of digital forensics relating to recovery of digital evidence or data from a mobile device . It differs from Computer forensics in that a mobile device will have an inbuilt communication system ( e.g. GSM ) and , usually , proprietary storage mechanisms . Investigations usually focus on simple data such as call data and communications ( SMS / Email ) rather than in @-@ depth recovery of deleted data . SMS data from a mobile device investigation helped to exonerate Patrick Lumumba in the murder of Meredith Kercher .

Mobile devices are also useful for providing location information ; either from inbuilt gps / location tracking or via cell site logs , which track the devices within their range . Such information was used to track down the kidnappers of Thomas Onofri in 2006 .

= = = Network forensics = = =

Network forensics is concerned with the monitoring and analysis of computer network traffic , both local and WAN / internet , for the purposes of information gathering , evidence collection , or intrusion detection . Traffic is usually intercepted at the packet level , and either stored for later analysis or filtered in real @-@ time . Unlike other areas of digital forensics network data is often volatile and rarely logged , making the discipline often reactionary .

In 2000 the FBI lured computer hackers Aleksey Ivanov and Gorshkov to the United States for a fake job interview . By monitoring network traffic from the pair 's computers , the FBI identified passwords allowing them to collect evidence directly from Russian @-@ based computers .

= = = Forensic data analysis = = =

Forensic Data Analysis is a branch of digital forensics . It examines structured data with the aim to discover and analyse patterns of fraudulent activities resulting from financial crime .

= = = Database forensics = = =

Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata . Investigations use database contents , log files and in @-@ RAM data to build a timeline or recover relevant information .

= = Education and Research = =

Academic centre of education and research in forensic sciences :

North America : Penn State University offers Security and Risk Analysis Major , Master of Professional Studies in Information Sciences , Master of Professional Studies in Homeland Security , and Ph.D. in Information Sciences and Technology in the digital forensics area .

= = Related journals = =

Journal of Digital Forensics , Security and Law
International Journal of Digital Crime and Forensics
Journal of Digital Investigation
International Journal of Digital Evidence
International Journal of Forensic Computer Science
Journal of Digital Forensic Practice
Small Scale Digital Device Forensic Journal