PILON

ZYBER & INSIG2

FUNDAMENTALS OF DIGITAL FORENSICS

LAW ENFORCEMENT WORKBOOK

PACIFIC ISLANDS LAW OFFICERS' NETWORK

The Pacific Islands Law Officers' Network (PILON) is a network of senior law officers from Pacific countries.

PILON has identified cybercrime as a strategic priority in its current Strategic Plan. The Cybercrime Working Group supports PILON to address this strategic priority and has developed this workbook for the benefit of course participants from PILON member countries. It forms part of broader efforts to tackle cybercrime from a regional perspective by developing knowledge of the fundamentals of digital forensics.

Members of the Cybercrime Working Group (as at September 2022) are:

Tonga (Chair)	**American Samoa**
Australia	**Cook Islands**
Fiji	**Federated States of Micronesia**
Nauru	**New Zealand**
Papua New Guinea	**Solomon Islands**
Vanuatu	

Acknowledgements

Participation in this course has been funded by the Australian Government through:

CYBER & CRITICAL TECH COOPERATION PROGRAM

This workbook supports the online course delivered by:

INSIG2

Zyber Global

This workbook includes significant contributions from the following agencies, from who permission should be sought before adapting any material:

CDPP Australia's Federal Prosecution Service

ODPP Solomon Islands

This workbook contains illustrations prepared by Think In Colour.

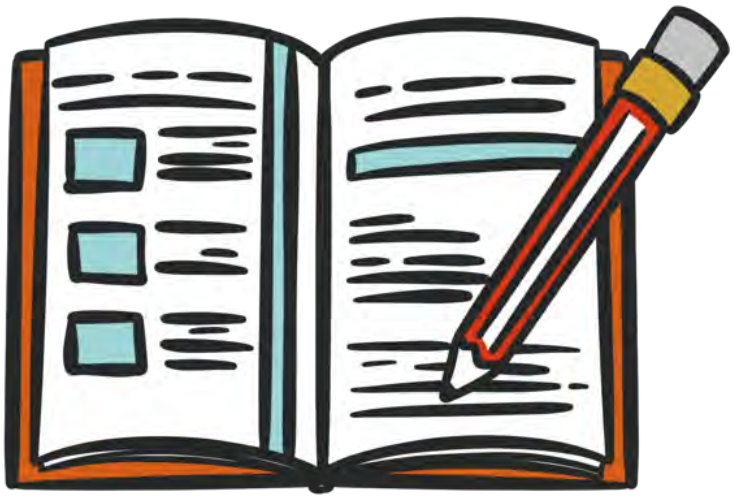
Australian Aid

This publication has been funded by the Australian Government through the Department of Foreign Affairs and Trade. The views expressed in this publication are the author's alone and are not necessarily the views of the Australian Government.

CONTENTS

Introduction: Course information

Who should use this workbook?



This workbook is intended for law enforcement officials, lawyers and public prosecutors to assist with understanding the basics of digital forensic investigations and related challenges.

When to use the workbook?

This workbook is intended to be used simultaneously with the online course. It is an excellent resource for those without stable internet connection or for those who prefer the hardcopy as it is a single download.

It accompanies and mirrors the content of the online course and contains the most important terms, phrases and definitions, along with statistics and examples relevant to the Pacific region. The workbook will be an aid during the quiz checkpoints, as well as after the course concludes. The notes page after each section allows the reader to add remarks to discuss with other participants during the course.

How is the workbook structured?

The workbook structure follows the chapter structure of the online course. The law course outline for law enforcement is available online at insig2-and-zyberglobal.learnworlds.com /course?courseid=**fundamentals-of-digital-forensics-for-le-agdpilon**, and the course outline for lawyers is available online at 'https://insig2-and-zyberglobal.learnworlds.com /course?courseid=**fundamentals-of-dfir'**. The structure of each course is a detailed breakdown of digital forensics methodology, covering all processes from defining and identifying digital evidence to presenting and testifying in court.

How can I get involved beyond the course material?

- **Weekly emails:** Look out for the weekly emails which highlight interesting issues raised in the course for this week, any relevant news items, or further reading
- **Discussion tab:** Have a look at the 'discuss' tab beside each page within the platform – you may wish to ask a question, make a comment, or simply react
- **Case study meetings:** There will be three case study meetings, approximately once every 2 weeks, starting halfway through the course. These will be an important time to network, discuss and meet industry professionals.

How can I get help or more information?

- ask the course facilitators using the pacific@ag.gov.au email below
- ask fellow participants within the online discussion tab or class meetings.

Who are the course contacts?

	Name	Role	Contact
Course facilitators	**Nicholas Wilson**	Legal Officer, AAGD	Pacific@ag.gov.au
	Lauren Murray	Senior Legal Officer, AAGD	
Course designers	**Krešimir Hausknecht**	Head of Digital Forensics Department, Insig2	Kresimir.Hausknecht@insig2.com
	Esther George	CEO, Zyber Global Centre	office@zyberglobal.com
Course sponsor contact	**Sasae Walter**	Coordinator, PILON Secretariat	coordinator@pilonsec.org

Chapter 1: Introduction to digital forensics

Branches of digital forensics

Digital forensics is a science that aims to collect, store, retrieve, analyse and document evidence that is stored, processed or transmitted digitally. It includes:

- Computer forensics
  - Dead box data
  - Live data
- Mobile forensics
- Cloud forensics
- Network forensics

Cybercrime versus cyber security

Cybersecurity and cybercrime are separate, but related concepts.

As we'll see in this chapter, **CYBERCRIME** is criminal activity where a computer or network is integral to, or the target of, an offence. It will often target individuals, their data or their reputation. On the other hand, **CYBERSECURITY** (also known as information technology security or electronic information security) involves preventing the technical exploitation of such vulnerabilities and mitigating the risk of such exploits occurring. In other words, cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

This course does not discuss cybersecurity, but better cybersecurity reduces certain kinds of cybercrime – so in some ways, the concepts of cybercrime and cybersecurity are opposite sides of the same coin.

Cyber-enabled versus cyber-dependent crimes

CYBER-ENABLED CRIMES are crimes committed in offline environments, for example, fraud, theft, sexual or harassment offences, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). Unlike **CYBER-DEPENDENT CRIMES**, they can be committed without the use of ICT. Two of the most widely committed instances of cyber-enabled crime relate to fraud and theft.

PILON MLA Handbook – Chapter 2.1

"Technology-enabled offences use the internet and ICT as a force multiplier. These crimes use the internet to increase the scale and reach of victims using computers, computer networks or other forms of information communications technology. Examples of technology-enabled offences include fraud, theft, sexual exploitation and harassment offences." (*read more on the PILON website*)

In contrast, **CYBER-DEPENDENT CRIMES** (or **DIGITAL CRIME** / **PURE CYBERCRIME**) includes crimes focused on offences against computer data or systems, unauthorised access, modification or impairment of a computer or digital system.

PILON MLA Handbook – Chapter 2.1

"Pure cybercrime offences differ from technology enabled crimes, as they require the use of ICT. That is, crimes against computers and information systems where the aim is to gain unauthorised access to a device or deny access to a legitimate user [...]. Other examples include hacking, the production and dissemination of malware for the purpose of criminal activity, botnets and phishing. (*read more on the PILON website*)

Summary of the differences

CYBER-ENABLED CRIMES	CYBER-DEPENDANT CRIMES
Use technology to enable offences which can also be committed in offline environments	Pure 'cybercrime' offences, made possible only by the technology itself
Examples of cyber-enabled crimes • electronic financial frauds • phishing scams • fraudulent sales • other criminal activities (e.g. drug dealing, human trafficking, economic fraud).	**Examples of cyber-dependent crimes** • spreading viruses and other malware • unauthorised modification or destruction of data (hacking) • distributed denial of service attacks
	

Chapter 1 Glossary of terms

CHILD ABUSE MATERIAL (CAM) – the term unifies a collection of illegal pictures/videos of underaged children.

FRAUD – wrongful or criminal deception intended to result in financial or personal gain.

MALWARE (malicious software) – any software that is intentionally designed to cause damage to a computer, server, client, or computer network. The most common types of malware are viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware.

Pacific Cyber Stat

"The ACSC observed over 1,500 cybercrime reports of malicious cyber activity related to the coronavirus pandemic (approximately 4 per day)."

ACSC Annual Cyber Threat Report 2021, page 10

PILON MLA Handbook – Chapter 2.2

"There is no single 'type' of cybercriminal. Historically, criminal prosecutions and investigations reveal that cybercrimes can vary significantly in terms of age, sophistication, resources, objectives and technical abilities."(*read more on the PILON website*)

Chapter 1 Other relevant terms

IDENTITY THEFT – the fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.

MALICIOUS HACKING – the gaining of unauthorised access to data in a system or computer in order to perform malicious activities which intention is to harm the data or system.

PLAGIARISM – the practice of taking someone else's work or ideas and passing them off as one's own.

RANSOMWARE – a type of malicious software designed to block access to a computer system until a sum of money is paid.

WANGIRI FRAUD – refers to the activity of calling a victim's mobile phone and hanging up after one ring, hoping the victim will return the missed call out of curiosity or courtesy. If the victim does, he or she unsuspectingly calls an expensive premium number

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

What happens when strong encryption becomes the norm? This topic was talked about in a recent Australian Strategic Policy Institute Report about the future of law enforcement assistance in an end-to-end encrypted world.

Further listening

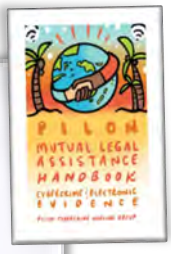
The Introduction to Digital Forensics in Real Life (DFIRL) Podcast – this is a true crime podcast hosted by Kim Bradley from Magnet Forensics, which explores real cases that were solved with the help of digital forensics.

Further resources

Registering for your free account PILON account today allows you to access the Members' Zone, containing exclusive members-only recordings within the PILON Cybercrime Working Group digital library.

Chapter 2: What is digital evidence?

What is digital evidence?



PILON MLA Handbook – Chapter 2

"Electronic evidence, also known as e-evidence or digital evidence is 'any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings."(*read more on the PILON website*)

Where can digital evidence be found?

Digital evidence can be found in many places, such as a computer hard drive, a mobile phone, and even a car. Digital evidence is commonly associated with digital crime. Different types of digital evidence can be found on:

- Computers
- Mobile devices
- Digital video and audio devices
- Network-based evidence
- Other electronic devices

Key concepts in defining sources of digital evidence

COMPUTERS AND LAPTOPS are electronic devices for storing and processing data according to instructions given by the user.

GAMING CONSOLES can be used for communicating with other players and can connect to the Internet. They are prone to similar forms of misuse and abuse as personal computers.

EXTERNAL DEVICES are crucial to be acquired since the bulk of evidence is often stored upon them. They are called external since they are physically not a part of the computer but can be plugged in, Data can be transferred to or from them and transmitted to another computer.

MOBILE DEVICES include tablets, smart home appliances, smart cars, etc. In other words, mobile devices are any devices running on a mobile operating system.

WEARABLE TECHNOLOGY or **WEARABLES** are smart electronic devices that can be incorporated into clothing or worn on the body as accessories. Wearables include activity trackers, smartwatches, body cameras for law enforcement, wearable technology for assisted living, and fashion electronics.

UNMANNED AIRCRAFT SYSTEMS (DRONES) are remote-controlled pilotless aircraft or small flying devices which store data in digital formats and have become a tool for criminal activities (causing drone forensics to become a new and important part of digital forensics).

NETWORK DEVICES (routers, HUBs, etc.) are electronic devices which are required for communication and interaction between devices on a computer network. Investigation of network devices is part of network forensics.

CLOUD is a general term for anything that involves delivering services over the internet.

PILON MLA Handbook – Chapter 2.4

"In many ways, electronic evidence is no different from traditional evidence (such as documents, photographs, witness testimony, and DNA)." (*read more on the PILON website)*

IN-VEHICLE INFOTAINMENT SYSTEMS/NAVIGATION SYSTEMS/GPS DEVICES – when talking about vehicles, location data is extremely important. It provides historical data to show where a vehicle was at specific times. This data also identifies areas frequently visited, new locations travelled, future plans to travel, and how long was a vehicle at a particular location.

IOT DEVICES is a relatively new area in information technology. An IoT device is a piece of hardware that transmits data from one place to another over the Internet.

SMART HOME AUTOMATION will control lighting, air conditioning, entertainment systems, and appliances. It may also include home security such as access controls and alarm systems. When connected to the internet, home appliances form an important component of the Internet of Things.

HOME INTELLIGENT PERSONAL ASSISTANT is a software agent that can perform tasks or services for an individual – based on commands or questions. Some virtual assistants can interpret human speech and respond via synthesised voices.

SMART APPLIANCES are used together to enable the concept of a smart environment. Such data contain valuable forensic information about events and actions occurring within a smart environment and, if analysed, can help breach security policies.

DIGITAL VIDEO RECORDING SYSTEMS are devices that record video in a digital format to disk drives, USB flash drives, SD memory cards or other storage devices.

CRYPTOCURRENCY is a digital asset, like money. There are hundreds of different cryptocurrencies on the market, the most popular one being Bitcoin. For the investigators, the most important evidence to find is a so-called, cryptocurrency wallet. A cryptocurrency wallet is a software program that stores private and public keys that enable users to send and receive digital currency.

PRACTICE TIPS

CDPP practice tips: connecting digital forensics to a person

Judy King (Principal Federal Prosecutor, CDPP)
Jon Emmett (Principal Federal Prosecutor, CDPP)

Proving ownership or use of a device:

1. Often, key evidence may be located on a device, but there is a question about whether the defendant owned or was the user of that specific device. For example, if a phone is located in a house in which multiple people live, the Prosecutor must establish that the defendant was the person who sent/received the relevant messages/calls, or took the relevant photographs.
2. To do this, Prosecutors can rely on a number of other pieces of evidence, such as where the device was located (for example, was it seized from the defendant's bedroom), the content of social messages (for example, messages between a defendant and a family member which refer to the defendant by name), and the content of photographs (for example, "selfies" of the defendant being taken on the phone).

Pacific Cyber Stat

"The ACSC observed approximately one quarter of reported cyber security incidents affected entities associated with Australia's critical infrastructure."

ACSC Annual Cyber Threat Report 2021, page 10

ODPP Solomon Islands' self-reflection

"Prosecutors should be trained to understand the functions of a digital machine, how to read it and the process of translating it into evidence to assist the court. The Prosecutor must know how to read and understand the footage's timing, and sequence before trial. If using Digital evidence to illustrate the theory of the case, it must align with the footage's sequence and timing."

Chapter 2 Glossary of relevant terms

LOGS – include files that record either events that occur in an operating system or other software runs or messages between different users of communication software.

LAN (Local Area Network) – a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

SET-TOP BOX – device that allows a digital signal to be received, decoded and displayed on a television.

CAMCORDER – a portable device used for video capture and recording.

CCTV (Closed Circuit Television) – also known as video surveillance; is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

VOLATILE (FLASH) MEMORY – memory storing data that gets lost when the computer is turned off.

BITCOIN – a digital or virtual currency created in 2009 that uses peer-to-peer technology to facilitate instant payments.

SOLOMON ISLANDS

A case study of digital forensics in action

What was the crime?

On one evening, gruesome murders were committed on a couple. The murders occurred within the confines of their business premises in Honiara. Their bodies were discovered two days after the killing. There was a public outcry, and police did not immediately establish any motive for the killing.

Where did the investigation lead?

Investigations led to the arrest of two persons, one of them was a security guard employed by the couple to look after their premises. He was on duty to look after the premises at the time the offence was committed. The arrest of the offenders was only made possible after witnesses saw the footage extracted from the CCTV installed in the premises and identified the security guard.

How was digital evidence obtained?

During their investigation, police investigators found that the couple installed surveillance cameras in their business premises where the incident occurred. The surveillance cameras were encrypted, and the Royal Solomon Islands Police Force could not extract the footage due to limited knowledge of the machine. The investigators consulted an IT expert, and the digital evidence was accessed and obtained through his expertise.

SOLOMON ISLANDS

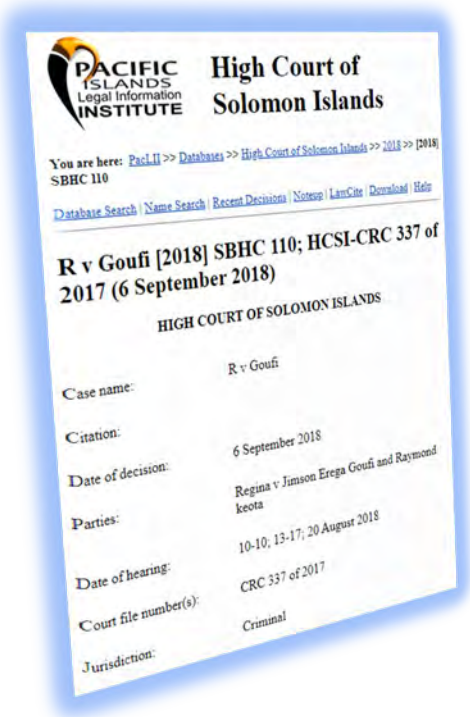
(continued)

How was digital evidence handled?

The extracted footage and still images were stored in storage devices and delivered to prosecutors who had carriage of the matter. The evidence obtained was disclosed to defence counsel as required. Police obtained a statement from the IT personnel who extracted the digital footage and image from the CCTV as evidence of how he obtained it.

What digital forensics did prosecutors rely upon?

The prosecution's case relied mainly on the footage and images taken from the surveillance cameras to prove the identity of the two defendants. The footage captured by the camera showed the two defendants attacking and killing the couple in this case.[1]


PACIFIC ISLANDS Legal Information INSTITUTE

High Court of Solomon Islands

You are here: PacLII >> Databases >> High Court of Solomon Islands >> 2018 >> [2018] SBHC 110

Database Search | Name Search | Recent Decisions | Noteup | LawCite | Download | Help

R v Goufi [2018] SBHC 110; HCSI-CRC 337 of 2017 (6 September 2018)

HIGH COURT OF SOLOMON ISLANDS

Case name:	R v Goufi
Citation:	
Date of decision:	6 September 2018
Parties:	Regina v Jimson Erega Goufi and Raymond keota
Date of hearing:	10-10; 13-17; 20 August 2018
Court file number(s):	CRC 337 of 2017
Jurisdiction:	Criminal

Hurdles overcome during trial

Identification was an issue during the trial. The prosecution overcame that hurdle through the digital evidence obtained from cameras installed in the premises where the offending occurred. Witnesses who were workmates of one of the defendants identified him as the security officer in that premises. He was one of the two attackers who killed the couple. The court found the defendants guilty of the murders. The digital evidence undoubtedly played a pivotal role in ensuring justice was served.

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

How could hard drive evidence support a conviction? Have a look at this 2019 story, where a NZ forensic investigator copied a hard drive as part of the investigation. In this case, someone was accused of planting a motion-activated camera in a unisex bathroom in the New Zealand Embassy in Washington DC.

Further listening

The Digital Detectives Podcast - hosted by two leaders in the cyber-security industry, the hosts (Nelson and Simek) invite digital forensic and computer security experts to enlighten listeners on the latest technology, cyber threats, and necessary security measures to keep online data secure.

Chapter 3: The digital forensic process

What is the digital forensic process?

The digital forensic process is a set of steps which need to be followed when handling digital evidence. It begins with the preparation required before arriving at the crime scene and ends in presenting the evidence in a court of law.

The process based on the ACPO principles

Worldwide, examiners usually follow guidelines issued by the United Kingdom Association of Chief Police Officers (ACPO), later on, the National Police Chiefs' Council (NPCC), for the authentication and integrity of evidence.

1 

ACPO Principle 1: That no action is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

2 

ACPO Principle 2: Where a person finds it necessary to access original data held on a digital device that the person must be competent to do so and able to explain their actions and the implications of those actions on the digital evidence to a court.

3 

ACPO Principle 3: That a trail or record of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third-party forensic expert should be able to examine those processes and reach the same conclusion.

4 

ACPO Principle 4: That the individual in charge of the investigation has overall responsibility to ensure that these principles are followed.

The digital forensic process visualised

1 PREPARATION

Before arriving at the crime scene and starting to identify digital evidence, investigators must prepare and have the required documentation (e.g. search warrant).

2 IDENTIFICATION

Identification is the first step in handling digital evidence (which involves both locations of potential digital evidence are identified, but also the scope of the crime in question.

3. PRESERVATION

Once the identification process is carried out, all identified devices should be transferred to the laboratory for analysis. Apart from the devices, the digital evidence first responder should also analyse any material that could be related to the crime, such as paper notes which can contain important information, like passwords.

4. ANALYSIS

Analysis is the in-depth examination of electronically stored information, to identify information that may support or contest matters in a civil or criminal investigation and/or court proceeding.

5. DOCUMENTATION

The best practice is to describe everything that was found and performed while doing the evidence analysis. When the analysis step is done, the evidence is preserved and stored in archive.

6. PRESENTATION

When presenting evidence to a court, everything from digital evidence seizure to the process of analysis must be explained, including how the extraction and analysis were performed, what was found, and what was concluded.

PRACTICE TIPS

CDPP practice tips: why the digital forensic process matters

Judy King (Principal Federal Prosecutor)
Jon Emmett (Principal Federal Prosecutor)

Continuity and integrity of the data:

1. If challenged, prosecutors must be able to prove that the device or digital evidence presented in Court is the same as the device or digital evidence seized during the investigation.
2. To assist in doing so, prosecutors should prepare a table for themselves, and potentially the Court if accepted, that summarises each step in the chain of custody, including, for example, the seizing officer, any other police officer involved in handling the evidence at the time of seizure, and how the device was stored.
3. Prosecutors must be in a position to demonstrate that the device was not interfered with while it was in storage, which might have affected the integrity of the data. For example, prosecutors may need to play to the Court the full video examination by police of the device, or tender evidence of property seizure records or exhibit custody records.

PILON MLA Handbook – Chapter 2.4

"The intangible nature of information stored electronically makes it even more volatile and fragile than traditional forms of evidence. When on devices with computer memory, it's volatile because it can easily be corrupted or destroyed." (*read more on the PILON website here*)

Chapter 3 Glossary of relevant terms

METADATA – files containing data that provide information about other data – in other words, "data about data".

ODPP Solomon Islands' self-reflection

"Investigators and prosecutors must ensure that the evidence is preserved while it is in their possession after it is acquired from the scene of crime. The original copy should never be altered. It must be preserved for production during the trial. Investigators and prosecutors should use a working copy in preparation for the trial.

What did last year's cohort say and learn about this chapter?

Topic: 'Digital Forensic Process'

Week 4 of the pilot course also covered the 'Digital Forensic Process'. In this video, we hear from Damian Rapira-Davies and Jon Peacock at the NZ Department of Internal Affairs on the topic (subscribe here for more).

Pacific Cyber Stat

"The only jurisdiction to list brute force activities within their most common cyber threats was Tonga."

PaCSON Annual Report 2020, page 17

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

What happens when the data to sort is too big? In this article by the FBI about investigating persons supporting foreign terrorists, an FBI agent explains that they needed the help of examiners from the New Jersey Regional Computer Forensics Laboratory (NJRCFL) to sort through and understand the evidence taken from the suspects' devices and computers.

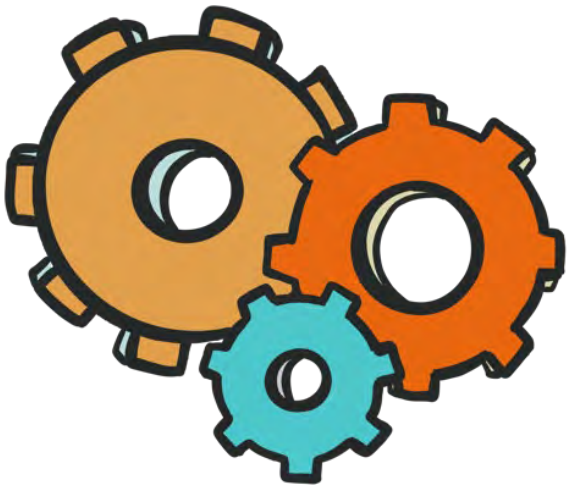
Further listening

The Forensic Focus Podcast – hosted by Christa Miller, this podcast discusses computer forensics and eDiscovery. The podcast is part of an organisation who support of best practice development within the digital forensics industry.

Chapter 4: Standard Operating Procedure

What is a Standard Operating Procedure (SOP)?

A standard operating procedure (SOP) is a set of procedures that need to be followed when investigating in a law enforcement context. Each company and law enforcement agency should have their own written procedure for all types of electronic devices.



ODPP Solomon Islands' self-reflection

"Police investigators should be educated on understanding, handling and preserving digital evidence. The Police should formulate a simple Standard Operating Procedure on handling digital evidence (procedure for acquisition protection and preservation). That SOP will be a guide to investigators who deal with digital evidence. It will show them the process or procedure to follow."

What are the general features of a SOP?

In general, a SOP should include (but is not limited to):

- the name of the SOP and an effective date
- purpose and scope of the SOP
- equipment calibration and similar preparatory steps, as well as references (such as equipment manuals, published procedures, journal references, etc.)
- any known limitations of the equipment, software or procedure

- a list of steps used in performing the task, including appropriate parameters or options to be used
- any additional information/materials the examiner needs to be aware of
- authorisation and approval information.

ODPP Solomon Islands' self-reflection

"Police should have a specialised computer forensic team instead of engaging outside IT technicians. Their 2020 SOP should be reviewed to include digital exhibits and how to deal with them."

What specific issues can a SOP help ensure?

A SOP can help ensure:

- compliance with local laws
- no deviation from standard process (which might otherwise jeopardise an investigation)
- integrity of fragile evidence (to eventually prove a case in court)
- that every iteration of analysis provides the same findings (by directing investigators to follow a repeatable and well documented set of steps)
- privacy and confidentiality
- determines the extent of authority to search
- an effective forensics investigation process.

Chapter 4 Glossary of relevant terms

ISO CERTIFICATION – is a set of standards (published by the International Organization for Standardization or ISO) that help organisations ensure they meet particular standards (including regulatory requirements) related to that product or service. The ISO certification is a written assurance that the product, service or system in question meets specific requirements.

SOLOMON ISLANDS

Solomon Islands: Profile of a SOP

In 2020 a revised Standard Operating Procedure on Exhibits was developed

In March 2020, the Royal Solomon Islands Police Force through the Crime and Intelligence Unit develop a Standard Operating Procedure[1] on Exhibits[1] to replace the one developed in 2005. The SOP defines the practice and procedures to follow when handling exhibits during investigations. The SOP also specifies certain people and their functions in managing exhibits.

While the SOP specifies the process and procedures when dealing with evidence or exhibits such as currency, drug, firearm, hazardous substance, high risk items and other valuables, it does not include digital items. The police use the conventional methods in dealing with digital items/exhibits.

Royal Solomon Islands Police Force

Crime and Intelligence

Governance Instrument

STANDARD OPERATING PROCEDURE
On
NCID - EXHIBITS

SOP Number: SOP/2020/001

Date of Original Issue: March 2020
Number of Pages:18

SOLOMON ISLANDS

(continued)

How does the Standard Operating Procedure relate to the case study?

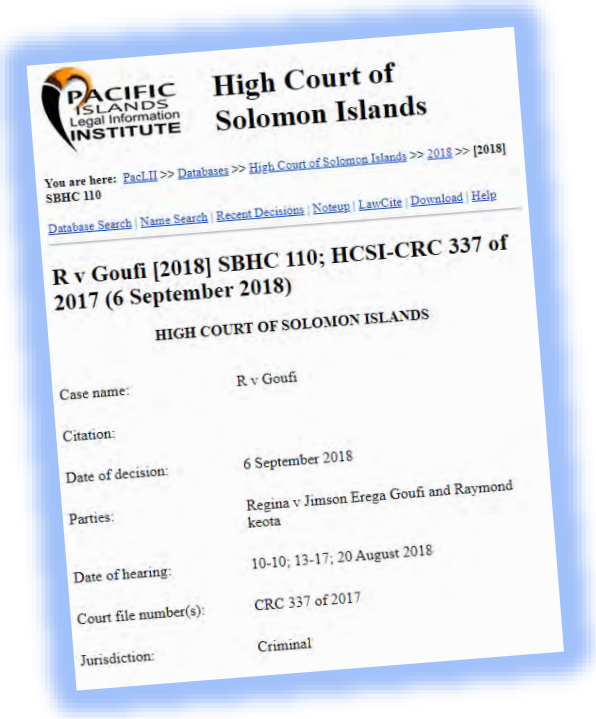
I. In respect to the case study (see page 17), police investigators obtained the CCTV tape or footage from the crime scene. The usual chain of custody was maintained to ensure that the evidence was not contaminated/damaged.

II. The SOP establishes the position of a registrar and his/her functions. The registrar conducts audits of exhibits. This includes recording who uplifted the footage from the crime scene, ensure that all details of tags, record sheets and all other items are secured. It should include how the footage moves from the police custody to the prosecution's office.

III. During the investigation, an IT expert was engaged to review the footage/image and extract the footage or image to a portable storage device.

VI. The original footage was retained by the police to preserve the integrity of the evidence but copies of the footage were transferred on to a memory stick as part of the police brief and forwarded to the prosecution for use during preparation and prosecution of the case.

VII. Upon receiving the police brief, the prosecution serves a copy of the disclosure on the defence.



PACIFIC ISLANDS Legal Information INSTITUTE

High Court of Solomon Islands

You are here: PacLII >> Databases >> High Court of Solomon Islands >> 2018 >> [2018] SBHC 110

Database Search | Name Search | Recent Decisions | Noteup | LawCite | Download | Help

R v Goufi [2018] SBHC 110; HCSI-CRC 337 of 2017 (6 September 2018)

HIGH COURT OF SOLOMON ISLANDS

Case name:	R v Goufi
Citation:	
Date of decision:	6 September 2018
Parties:	Regina v Jimson Erega Goufi and Raymond keota
Date of hearing:	10-10; 13-17; 20 August 2018
Court file number(s):	CRC 337 of 2017
Jurisdiction:	Criminal

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further listening

For those who want to learn more about the into technical details, the Digital Forensic Survival Podcast is hosted by a computer forensic analyst with over 13 years of investigative experience. This podcast is for the very technically inclined and information security professionals! Listen to talk about computer forensic analysis, techniques, methodology, tool reviews and more. There's over 300 episodes, so there's sure to be something there for you.

Pacific Cyber Stat

"Cybercriminals have created several fake Facebook profiles of "Barry Whiteside", Governor of the RBF [which are connected with] fake RBF approvals for victims to remit funds to secure proceeds of fake lotteries, investments and loans [...] the letterhead and logo of the RBF has been used by criminals."

Reserve Bank of Fiji Press Release No 19/2016

Chapter 5: Identifying digital evidence

Identifying digital evidence

As a general principle, when arriving at the crime scene, investigators should search for all the devices that store data in digital form, that can connect to the Internet or transmit digital data.

Examples of devices containing digital evidence

As discussed in Chapter 2, examples of these devices include:

Device Category		Examples
	**Computers**	Desktops, laptops and even gaming consoles
	**Mobile devices**	Tablets, smart home appliances, smart cars
	**Digital video and audio devices**	Disk drives, USB flash drives, SD memory cards or other storage devices
	**Network-based evidence**	Routers, HUBs
	**Other electronic devices**	Activity trackers, smartwatches, body cameras for law enforcement, wearable technology for assisted living, and fashion electronics, unmanned aircraft systems (drones), in-vehicle infotainment systems/navigation systems/GPS devices, smart home automation systems/assistants and smart appliances

PRACTICE TIPS

CDPP practice tips: when sensitive evidence is identified

Judy King (Principal Federal Prosecutor)
Jon Emmett (Principal Federal Prosecutor)

Sensitive evidence

1. Prosecutors should be mindful to ensure that sensitive evidence is quarantined and not disclosed in a brief of evidence. Examples of sensitive evidence includes child abuse material (textual, videos and photos) or offensive material.
2. Prosecutors should make such material available to defence representatives for inspection to ensure that there is full and proper disclosure, to guarantee a defendant's right to a fair trial.

ODPP Solomon Islands' self-reflection

"After securing the crime scene, the investigators/their superiors should identify the type of digital evidence that is required or has the potential to assist the Police in solving the crime. This should include identifying, recognising, and documenting potential digital evidence at a scene. The process should identify digital storage media and processing devices that may contain evidence relevant to the Police to assist them in their investigation."

"

PILON MLA Handbook – Chapter 2.4

"If electronic evidence is to be introduced as 'evidence' in legal proceedings the court must be satisfied the evidence has not been altered or changed in any way from the time it was obtained." (*read more on the PILON website*)

Cause to seize computers

Cause to seize computers and related evidence might include:

- The computer is contraband or used in the commission of a crime. The computer system(s) contain evidence of a crime.
- A computer is a tool of the offence.
- The computer is both the instrument and storage device of a crime.

PRACTICE TIPS

CDPP practice tips: circumstantial digital evidence

Judy King (Principal Federal Prosecutor)
Jon Emmett (Principal Federal Prosecutor)

Assessing weight:

1. It is a common misconception that circumstantial evidence is somehow inherently of less weight than other sorts of evidence. In reality, most cases mostly involve circumstantial evidence, in particular, any inference of what was in a defendant's mind is almost invariably a matter of circumstantial evidence.
2. Circumstantial evidence is strengthened by assessing it in the context of the overall prosecution case, including considering other pieces of circumstantial evidence. Often a device will contain large amounts of data and metadata that a prosecutor can rely on to strengthen the evidence. For example, in most cases, a prosecutor can rely on the metadata of specific photograph, which may show the date and time it was taken, the location it was taken, and the device used to take it.

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

What happens when the US Federal Bureau of Investigation (FBI) can't access two encrypted and locked phones (and the owner is dead?) Well, the FBI. asked Apple to help. Commentators thought it could reignite a fight between the Silicon Valley giant and law enforcement over access to encrypted technology. Do you want to guess what Apple then told the FBI?

Further listening

The 13Cubed YouTube Channel is a side project maintained by Richard Davis. This channel covers information security-related topics including Digital Forensics and Incident Response (DFIR) and Penetration Testing, as well as tutorials and overviews of various apps and scripts Chris has written.

Chapter 6: Digital evidence preservation

Digital evidence preservation

To start the search, a search warrant must be issued. All of the evidence must be properly bagged and tagged before arriving at a forensic laboratory.

Search warrant

A search warrant is a document signed by a magistrate giving law enforcement officers the authority to search a specified place for specific items that are particularly described in the warrant.

The number one rule in warrant execution regarding digital, especially computer evidence, is move everyone away from the area where the device is located … **DO NOT ALLOW ANYONE (ESPECIALLY THE SUSPECT) TO TOUCH THE KEYBOARD**.

Procedures at the crime scene

When at the crime scene, these procedures should be adapted as necessary:

- Ensure the safety of all the individuals at the scene. Protect the integrity of evidence.
- Evaluate the scene and formulate a search plan. Identify potential evidence.
- All potential evidence should be secured, documented, and photographed.
- Conduct interviews.
- Any item to be removed from the scene should be properly packaged and secured.

Pacific Cyber Stat

"Kiribati has seen a surge in usage of the internet by the general population during the COVID-19 pandemic. Kiribati have also observed an increase in the number of scams during this time, including pyramid schemes and social-engineering scams."

PaCSON Annual Report 2020, page 17:

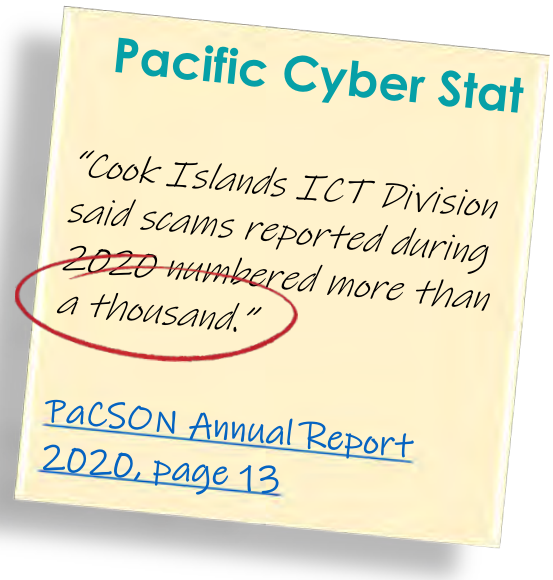
ODPP Solomon Islands' self-reflection

"Protocols (Crime scene) - Police should have protocols for dealing with digital evidence at crime scenes. This is to avoid errors, oversights or damage to the evidence. The investigator responsible for securing a crime scene, whether first responders or digital evidence examiners, should be trained to follow accepted protocols. These protocols should prevent contamination or damage to evidence."

BAG & TAG EVIDENCE - All the evidence collected from a crime scene needs to be taken care of properly, meaning it should be correctly tagged and placed in specific bags before reaching the forensic laboratory.

STORAGE MEDIA - In computers, a storage medium is any technology – including devices and materials – used to place, keep and retrieve electronic data. It refers to a physical device or component in a computing system that receives and retains information relating to applications and users.

WRITE BLOCKING - A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data.



Size and types of storage media

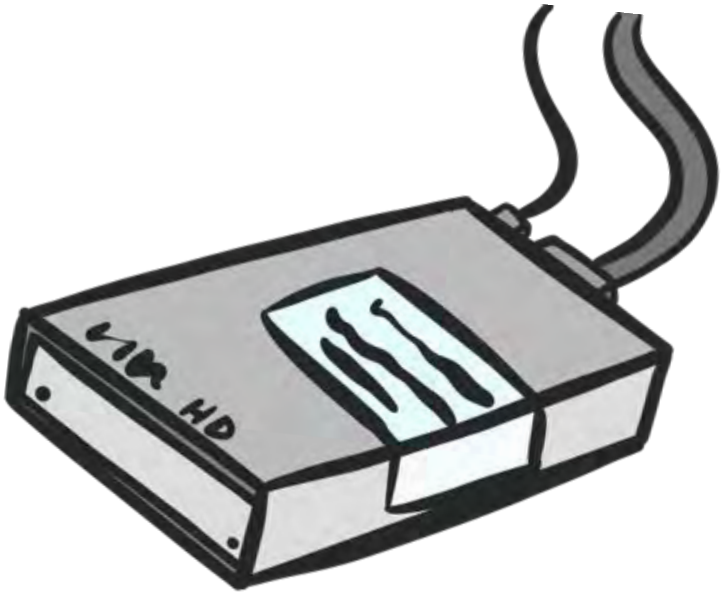
A HARD DISK DRIVE (HDD) provides a high-capacity alternative to magnetic storage media

- **SOLID STATE DISKS (SSD)** store data with the use of flash-memory chips (called NAND flash memory).
- **DIGITAL VERSATILE DISC** or **DIGITAL VIDEO DISC (DVD)** is a digital optical disc storage format used to store high capacity data, like high- quality videos and movies.
- **COMPACT DISCS** hold 700MB of data (equivalent to 80 minutes of audio, hundreds of high-quality digital images, and small video files).
- **BLU-RAY DISC** contains 25 GB per layer. Blu-ray is similar to normal DVD or CD in size dimension but in space, and memory is larger than DVD.
- A **USB FLASH DRIVE** is a device used for data storage that includes a flash memory and an integrated Universal Serial Bus (USB) interface.
- A **SMALLER SIZE MEMORY CARD** is a device used for data storage.

Pacific Cyber Stat

"The FIU has also recently become aware of an increase in the number of reported cases of fraud and theft of money from bank accounts by means of unauthorised access to internet banking facilities. [...]. They are usually foreign nationals who operate from outside of Fiji."

Reserve Bank of Fiji Press Release No 24/2011



STERILIZATION - Sterile media is defined as magnetic media on which every byte has been overwritten in order to eliminate any data that previously existed on the media. This process is also called "wiping" or "sterilising".

VALIDATION - In the realm of computer forensics, "validation" means the process of verifying that something works as it is expected to work.

HASHING - The process of transforming any given key or a string of characters into another value. As stated earlier, the forensic examination should never be performed on the original evidence, if that is possible. A forensic clone is an exact bit-by-bit copy (1 or 0) of the original media. The process of creating a forensic copy or image is called imaging. The most common hash functions used in digital forensics are Message Digest 5 (MD5), and Secure Hashing Algorithm (SHA) 1 and 256.

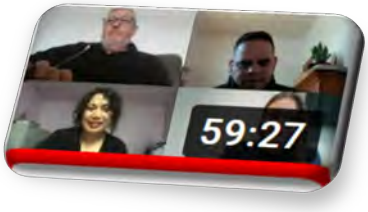
ENVIRONMENTAL CONTROL -Creating a forensically sound examination environment involves ensuring the working environment is completely under the control of the forensic examiner at all times.

CHAIN OF CUSTODY - The chain of custody in digital forensics can also be referred to as the forensic link, the paper trail, or the chronological documentation of electronic evidence. It indicates the collection, sequence of control, transfer, and analysis.

ODPP Solomon Islands' self-reflection

"After the relevant evidence is identified, the procedure for collecting the evidence must be clearly set out. The evidence collected should be appropriately recorded and packaged before it is removed from the scene of the crime."

What did last year's cohort say and learn about this chapter?



Topic: 'Digital Evidence Preservation'

This video relates to the topic of digital evidence preservation, as considered by last year's cohort. Our expert speakers, Damian Rapira-Davies and Jon Peacock from the New Zealand Department of Internal Affairs share their knowledge with the cohort (subscribe here for more).

Chapter 6 Glossary of relevant terms

FARADAY BAG – a bag made of a special material that blocks electromagnetic signals. It is used to hold devices, such as mobile phones, in order to repel outside signals from interfering with the contents of the device.

ARSON CAN – an arson can is a clean, empty paint can. These containers can be found in hardware or home improvement stores.

WIPING – the process of unrecoverably deleting all the data from a digital evidence.

CRYPTOGRAPHY – the study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents.

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

What happens when an important 'address book' to someone's IP addresses fails? It happened to Facebook recently (you might have noticed) – and it caused a lot of drama.

Further reading

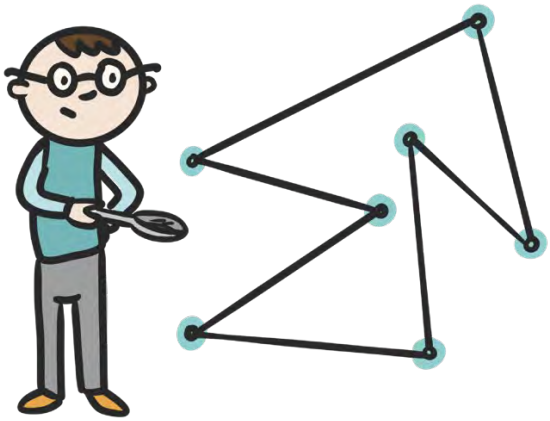
If you want to learn more behind some murky digital interactions, take a look at this recent ASPI report on the 'shadow online influence-for-hire economy'.

Further reading

Here's another story about why some people use Virtual Private Networks (VPNs), and why it's causing a headache for another big company, Netflix.

Chapter 7: Analysis and Documentation

What do examiners do in this phase?



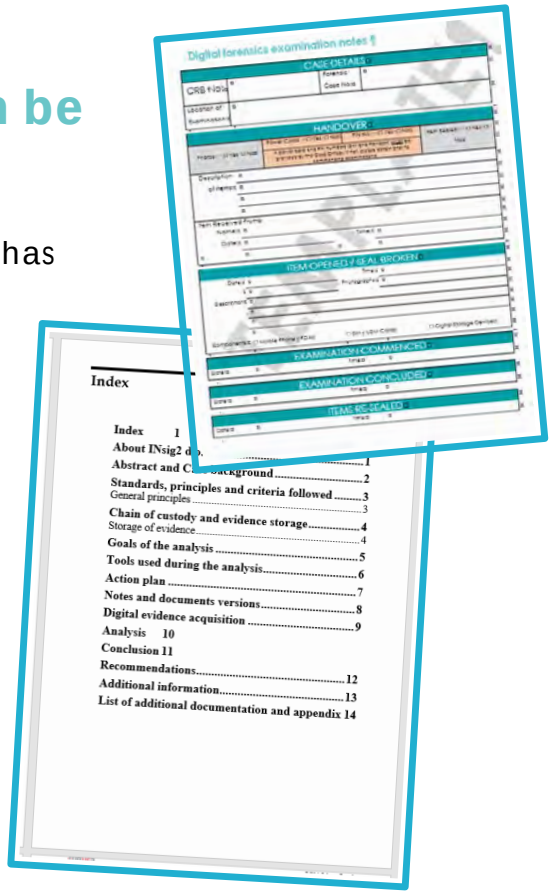
In the analysis phase, examiners connect all the dots and paint a complete picture in order to get to the conclusion of the case.

What kind of questions are answered?

Examiners answer questions like who, what, when, where, and how. They try to explain which user or application created, edited, received, or sent each item, and how it originally came into existence. The examiner may use specialised forensic tools to perform specific actions and help find or recover evidential information, e.g. deleted files, certain images and media files.

How might evidence examination be documented?

An example of digital forensics examination notes has been included at the end of this workbook.



What does the analysis lead to?

In Chapter 9 we'll discuss reporting, which is what analysis and documentation ultimately supports. An example of a written report is attached at the end of this workbook.

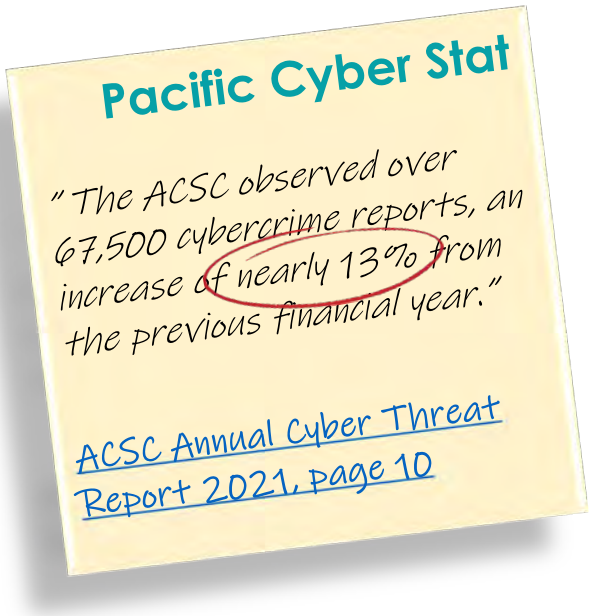
Chapter 7 Glossary of relevant terms

UNSTRUCTURED DATA – information that either does not have a pre-defined data model or is not organised in a pre-defined manner.

URL (Uniform Resource Locator) – a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. In web browsers, URLs are mostly displayed above the page in an address bar.

CRYPTOGRAPHIC KEY – a string of data that is used to lock or unlock cryptographic functions, including authentication, authorisation, and encryption.

EMAIL ADDRESS – identifies an email box to which email messages are delivered. It is made up of a local-part (e.g. john.smith), an @ symbol, and domain (e.g. gmail.com).



.

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

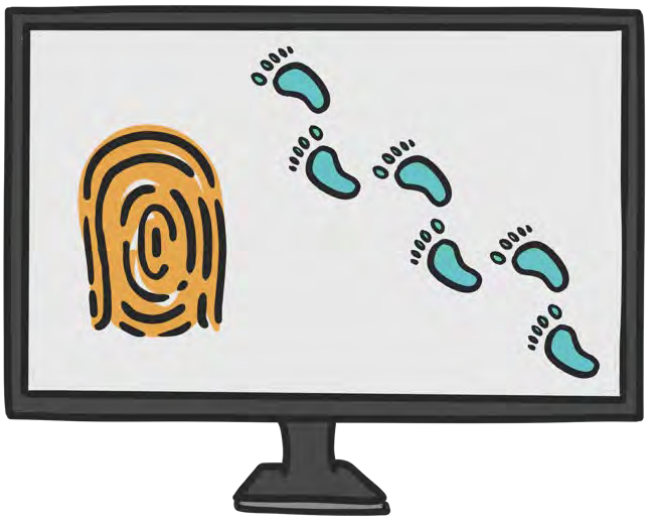
How have hackers gotten away with some of the biggest cloud data breaches this century? This article gives a summary of the top seven. You might even discover your data has been affected!

Further reading

Learn about the The challenge of sharing information and intelligence in the Pacific in a recent report issued by the Pacific Fusion Centre's Special Report. You can also see their website at www.pacificfusioncentre.org

Chapter 8: Computer forensics – introduction

Defining computer forensics



Computer forensics is a branch of digital forensic science relating to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound way with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about digital information.

How can a computer be involved in crime?

A computer can be involved in crime in three different ways:

1.

A computer is the target of a crime

2.

A computer has been used as a tool in the commission of a crime

3.

A computer has been used in an incidental manner (e.g. it has been used to store a record)

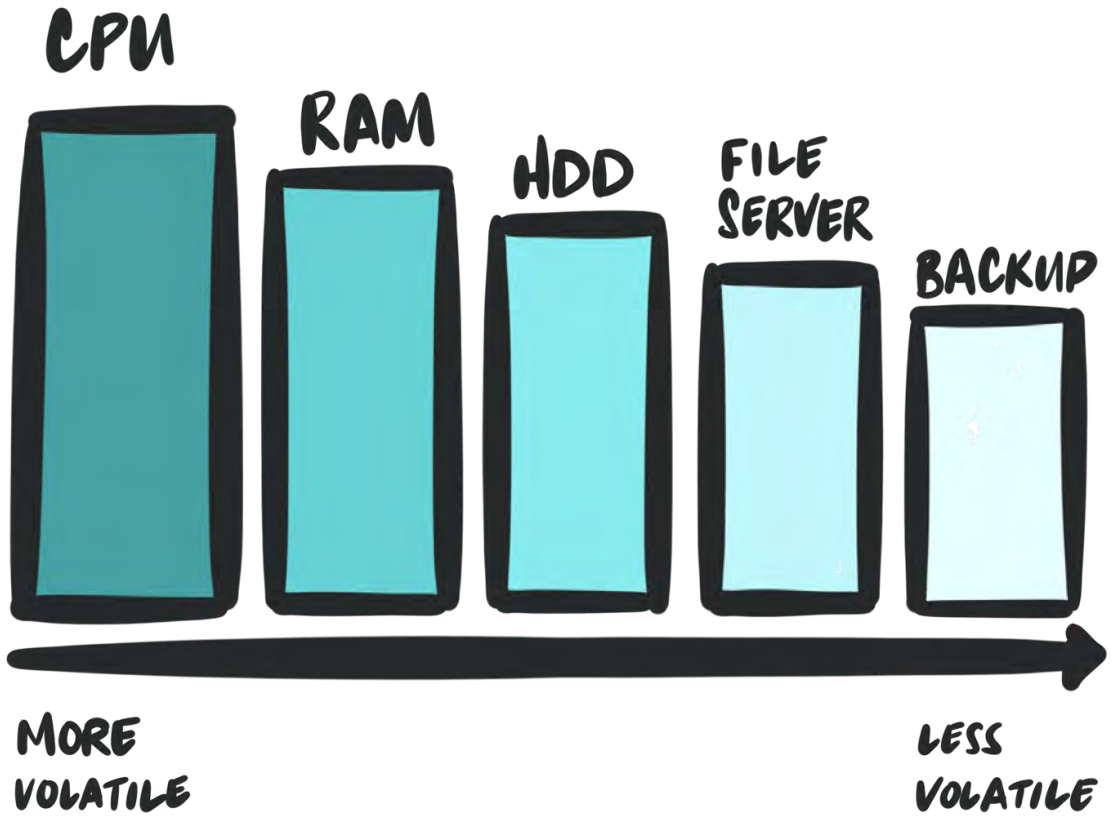
Dead box vs live data forensics

The collection of potential evidence in real-time is captured by the term **LIVE DATA FORENSICS**. In contrast, **DEAD BOX FORENSICS** refers to the analysis of the data "at rest" (data which reached a destination and is not being accessed or used).

Two main rules when coming across a computer

1. If the computer is turned off, leave it off.

2. If the computer is turned on, it depends, but best practice would be to create a dump of its Random-Access Memory (RAM) (a lot of useful information can be found in RAM – passwords, encryption keys, pictures, recent files, network connections, running processes, malware information, etc.).



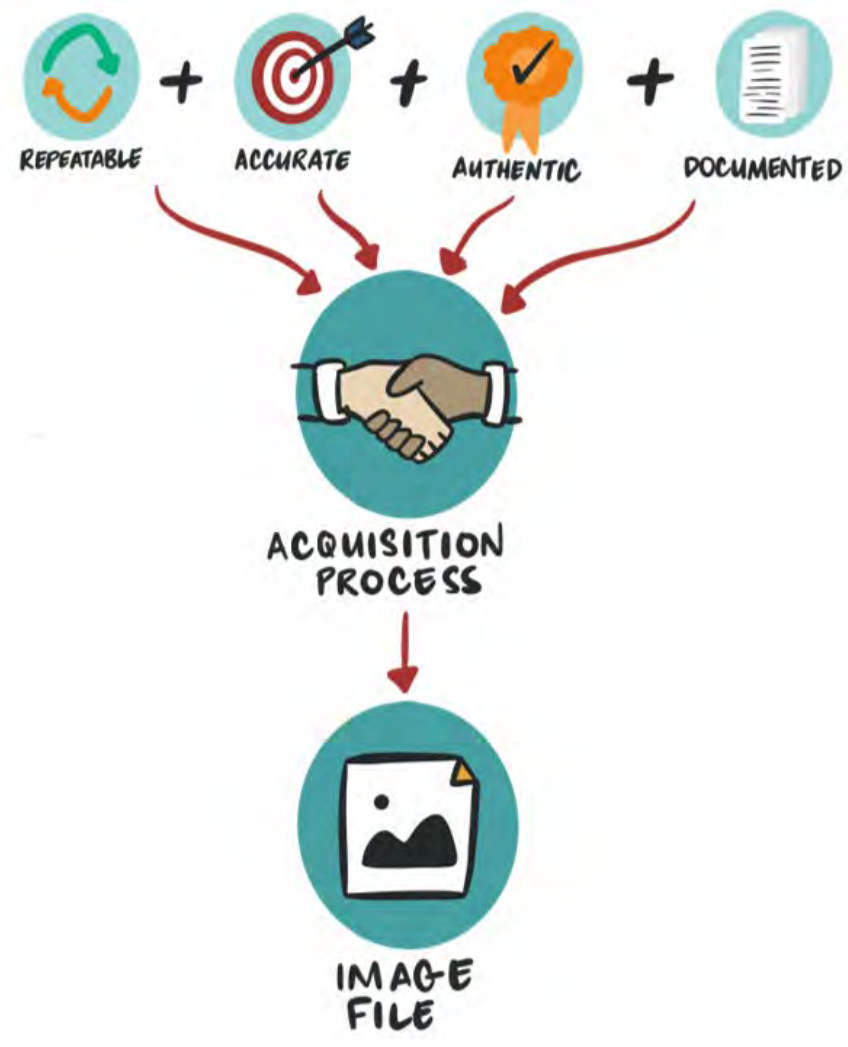
Encryption and decryption

In an **ENCRYPTION** scheme, the intended information or message, referred to as a plain text, is encrypted using an encryption algorithm. The reverse process is called **DECRYPTION** and it is used for decoding the message.

Acquiring digital evidence

After the evidence is identified and seized, the next step is to create a forensic copy, which can be logical, file-based or physical.

Extraction method	What does this actually extract?
Logical copy	extracts user data from a device, and typically only takes data residing on their reserved space on a hard drive, called allocated data (while physical takes both allocated and unallocated data)
File-based copy	extracts the file system of the device, user data, mobile application data, and possibly hidden files
Physical copy	extracts a bit-by-bit binary image of the flash memory – including the file system, user data, hidden files, unallocated space, and can contain passwords. In other words, the physical image will also contain deleted files. Unallocated data resides in "free" space on the disk after being deleted and is available to store new data. Old data that was residing there would then be overwritten by the new data.



A quick summary of concepts in this chapter

Acquisition format

Physical	Logical	File based

Forensic imaging tools

Open-source	Free	Commercial

Data categories that may contain digital evidence

Active data	Archival data	Latent data
Log files, printer spooler, cookies, history files, temporary files, hidden files, databases	Address books, email, SMS, multimedia files, calendars, spreadsheet files, documents, encrypted files.	Not readily visible and specialised tools are needed to see this type of data (such as deleted files or kinds of metadata)

EVIDENCE PROCESSING – is a process in which a forensic tool reads data from the imported evidence file and presents them in a user-friendly way (this process is also called parsing or decoding).

CARVING – the forensic technique where tools are used to try recovering deleted files from unallocated space

FILE SYSTEM – controls how data is stored and retrieved from a device. Microsoft Windows employs two major file systems – NTFS and FAT.

Pacific Cyber Stat

"FIU's intelligence outputs are disseminated to, and used by, the Cybercrime Unit. In 2016, 58 case dissemination reports involving $60.4 million were reported by the Fiji FIU to the Fiji Police Force, including cybercrime."

Reserve Bank of Fiji Press Release No 10/2017

What did last year's cohort say and learn about this chapter?

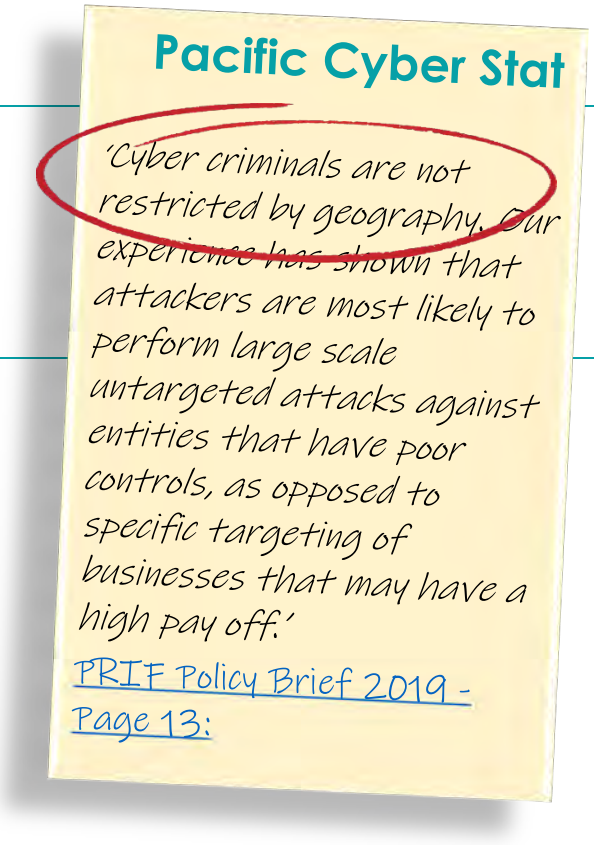
Topic: 'Computer Forensics Introduction'

Superintendent Kalisi Tohifolau and CERT representative Siosaia Vaipuna join us in this video to share their knowledge about computer forensics and provide insight into how police and the Computer Emergency Response Team work together in the Kingdom of Tonga (subscribe here for more).

Windows artefacts

Records are automatically generated and saved by the Windows operating system as a result of user interaction with the computer. A summary of these records, or 'artefacts' is below:

Artefact	What it is it?	Further details on where to find this artefact
User profile	Contains all configuration settings and files for each individual user account.	• Location of profile folders on Windows XP, WinNT and Win2000 is: C:\Documents and Settings\%UserName% • The location of profile folders on Windows Vista, 7, 8, and 10 is: C:\Users\%UserName%
Windows Registry	Central hierarchical database used in Windows to store information that is necessary to configure the system for one or more users, applications, hardware devices, and the overall functionality of the Windows Interface.	• \Windows\System32\config\SAM • \Windows\System32\config\SECURITY • \Windows\System32\config\SOFTWARE • \Windows\System32\config\SYSTEM • NTUSER.DAT
Recycle Bin	Temporary storage location from where items can be restored, individually deleted, or completely emptied.	
Event Logs	Used to monitor and troubleshoot the operating system. Windows event logs are categorised into 3 classes: application, security, and system.	



Chapter 8 Glossary of relevant terms

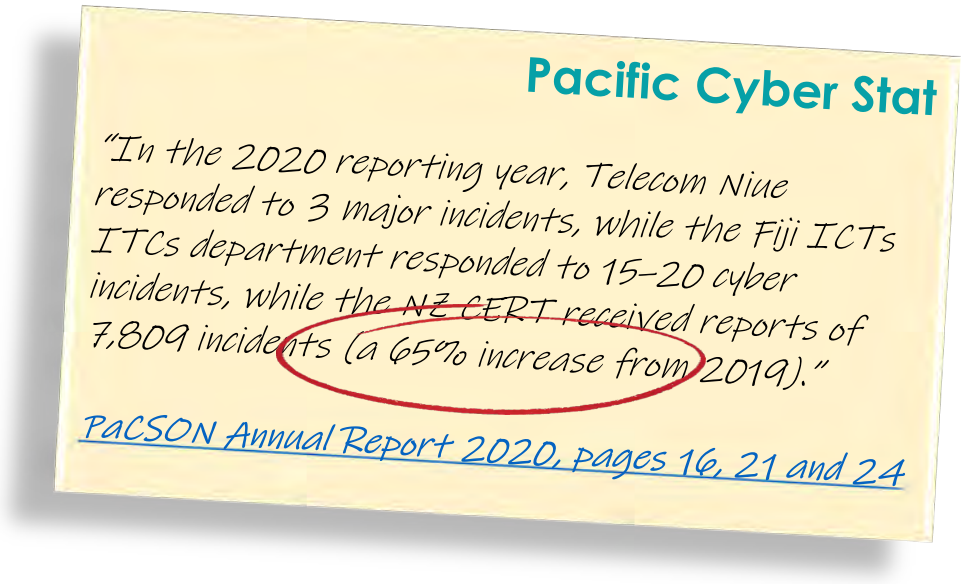
BRUTE FORCE – a type of attack on users' passwords; consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly

MBR (MASTER BOOT RECORD) – the most important file of the FAT files system; holds information on how the logical partitions, containing file systems, are organized on the medium.

SLACK SPACE – refers to the storage area of a hard drive ranging from the end of a stored file to the end of that file cluster.

JOURNALING FILE SYSTEM – a file system that keeps track of changes not yet committed to the file system's main part by recording the intentions of such changes in a data structure known as a "journal". Such files can be helpful in case of a system crash or power failure as they can be brought back online more quickly with a lower chance of being corrupted.

CLUSTER – a group of sections (the smallest unit that can be accessed on a storage device, like an HDD or SSD) that make up the smallest unit of disk allocation for a file within a file system. In other words, a file system's cluster size is the smallest amount of space a file can take up on a computer.



Chapter 8 Glossary of relevant terms (continued)

RAM (RANDOM ACCESS MEMORY) – a form of computer memory, typically used to store working data and machine code. It is considered volatile, as it requires power for the data to remain accessible.

CPU (CENTRAL PROCESSING UNIT) – the main processor within a computer that executes instructions that make up a computer program.

ALLOCATED DATA –data residing on their reserved space on a hard drive.

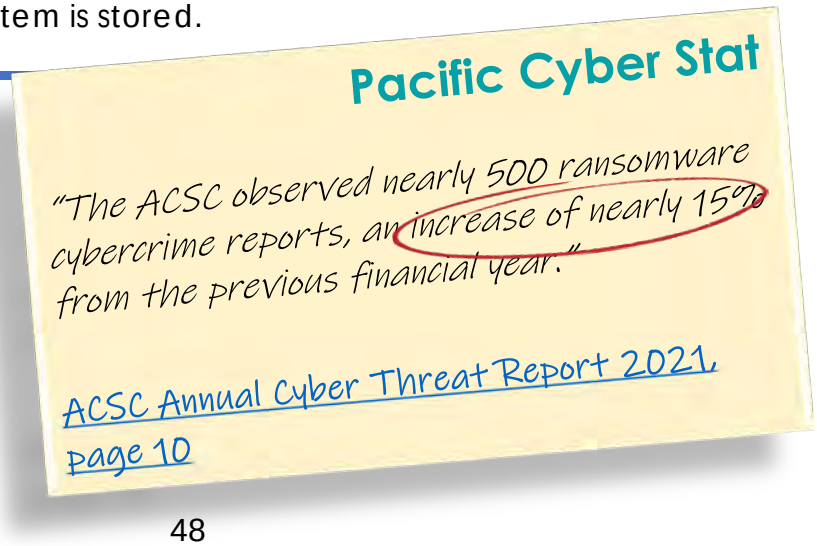
UNALLOCATED DATA – data residing in 'free' space on the disk after being deleted. Unallocated space is available to store new data even though it may contain old data which would then be overwritten by new data.

PARTITION – a section of the hard drive that is separated from other segments. Having multiple partitions enables users to divide a physical disk into logical sections (e.g. allowing multiple operating systems to run on the same device).

NTFS (NEW TECHNOLOGY FILE SYSTEM) – a file system first introduced by Microsoft in 1993. It is the most common file system for the end-user computers based on Windows operating systems.

FAT (FILE ALLOCATION TABLE) – a file system developed for hard drives that originally used 12 or 16 bits for each cluster entry into the file allocation table. It is often found in flash memory, digital cameras, and portable storage devices.

MFT (MASTER FILE TABLE) – a file in which information about every file and dictionary of an NFTS file system is stored.



NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further resources

Have you ever considered subscribing to PILON's YouTube Channel (click here for a direct subscription link). The channel includes recordings of the class meetings from the intermediate digital forensics course (as well as last year's fundamentals cohort).

Further discussions

Did you know there's a Facebook group where people discuss digital forensics? This page for people working within and interested in digital forensics. Group members often post articles, questions and comments on developments in digital forensics. Have a look, there might be a question you hadn't thought of!

Chapter 9: Mobile Forensics

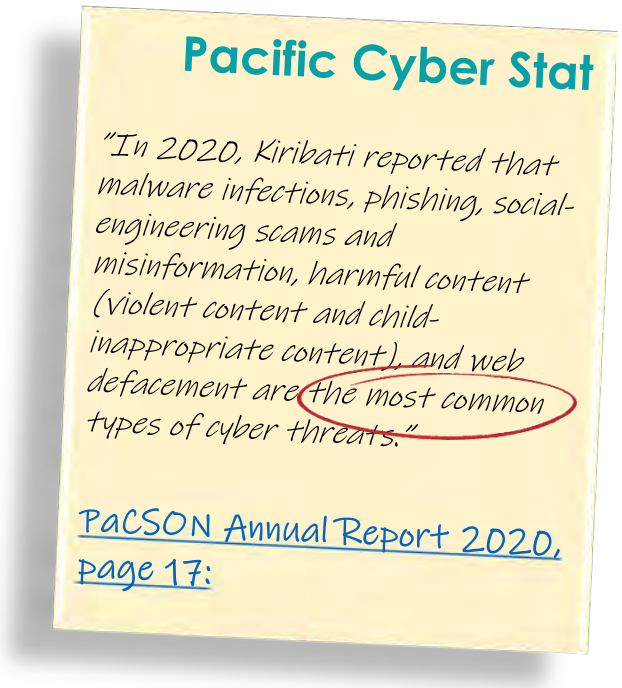
MOBILE FORENSICS is a branch of digital forensics relating to the recovery of digital evidence or data from a mobile device under forensically sound conditions.

Most mobile devices used worldwide are mobile phones. They can be divided into 5 different categories:

- legacy phones
- feature phones
- smartphones
- tablets
- clone phones (different in build but same appearance as a smart phone brand)

CDMA NETWORKS – these are the networks which connect to the handset. They use different methods to allow multiple callers access to single voice radio waves. CDMA networks do not require (but may have) a SIM card as the network connects to the device and the subscriber details are contained in the handset.

GSM SYSTEM – the most common system in use globally. GSM networks connect to the user's SIM card and require a SIM card, without which they cannot operate.



General principles when collecting mobile forensics

General principles apply and should be followed when collecting digital evidence from a mobile device. Some of the protocols that should be followed are:

1. if an investigator reasonably believes that digital devices are involved in the crime, take immediate steps to preserve the evidence
2. consider the legal basis needed to seize the digital device (such as a search warrant, consent, etc.)
3. do not search or access the contents of the digital device without applying digital forensic best practices to maintain the integrity of the data and admissibility of evidence – accessing files on the device can change or destroy data that destroys the value of the digital evidence.

Importance of network denial

Network denial is where a mobile device is prevented from connecting to the network. There are numerous reasons why the network denial of mobile devices is so important. From a compliance perspective, there may be legislative reasons (as well as consistency with the ACPO guidelines), and from a technical perspective, it is because of the possibility of losing SIM card data and handset data.

What are some network denial options?

- Faraday cage
- Airplane mode
- SIM clone (does not cover Wi-Fi)
- Signal jamming device
- Faraday bag, box or a tent

Extraction image types

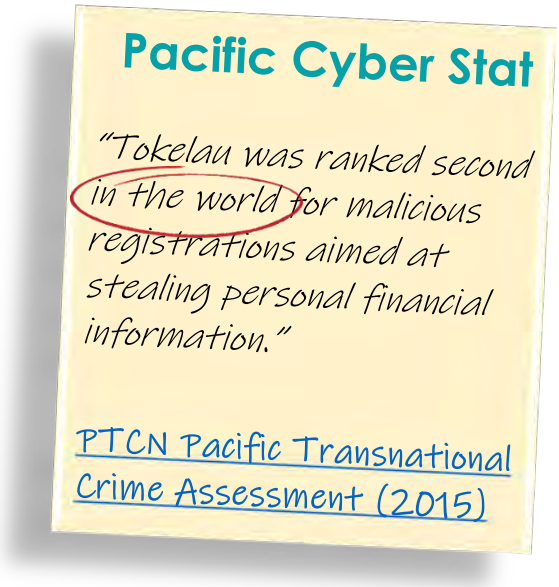
As we looked at in the previous chapter, extraction images offered by forensic tools offer can be generally divided into three categories – logical extraction, file system, and physical extraction (ie the same as computer forensics):

Extracted image types	What does this target?	Examples of data extracted
Logical	extracts user data from a mobile device	SMS, contacts, call logs, media, audio
File System	extracts the file system of the device, user data, mobile application data, and possibly hidden files	SMS, contacts, call logs, media, audio, files, **hidden files**
Physical	extracts a bit-by-bit binary image of the flash memory – has the file system, user data, hidden files, unallocated space, and can contain passwords	SMS, contacts, call logs, media, audio, files, hidden files, **deleted data**

Extraction method types

In general, extraction methods can be divided into five categories. Methods are listed starting from less technical, invasive, time-consuming, and forensically sound

Least invasive, time-consuming and forensically sound		→		Most invasive, time-consuming and forensically sound	
Manual extraction	Logical extraction	File system extraction	Physical extraction	Chip-off and JTAG	Micro read



Limitations for mobile forensics investigators

Limitations for mobile forensics include:

- big competition and no cooperation between mobile device manufacturers
- number of different types of phones
- many different charging connectors
- other languages or non-ASCII characters
- hundreds of device manufacturers
- cloud storage
- two factor authentication
- encryption
- damaged devices
- locked devices
- unsupported devices.

What did the Intermediate cohort say about mobile forensics?

Topic: Digital Forensics and IT Investigation Unit with the Fiji Police Force

In this video last year's cohort hears from Corporal Savenaca Siwatibau, Digital Forensics and IT (Fiji Police)Investigation Unit, Fiji Police Force about how they approach digital forensics (subscribe here for more).

Chapter 9 Glossary of relevant terms

GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS) – a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets.

CDMA (CODE-DIVISION MULTIPLE ACCESS) – a mobile phone service technology which is, opposed to GSM, primarily used in the United States of America and parts of Asia by other carriers.

FDE (FULL DISK ENCRYPTION) – the encryption of all data on a disk drive, including the program that encrypts the bootable Operating System (OS) partition.

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

What kind of footprint might a mobile leave? In this recent murder trial, a court looked at mobile phone data which showed the accused was close to the victim's home.

Further reading

For a snapshot of mobile device forensics trends, have a read of this report from the Australian Institute of Criminology.

Further reading

Reminding us how important phones are to investigations, UK Police have been joined by two dogs trained to sniff out technology including SIM cards.

Chapter 10: Reporting

Defining reporting

At the conclusion of the analysis, the examiner generates a final report. Forensic reports can be divided into written and tool-generated reports. Those reports are written to provide details to the reader on what was done and what was found.

Tool generated reports

All major forensic tools have the option to generate a report. Such reports contain tool details (name and version), extraction information, operating system information, extracted data by categories (media, contacts, emails, SMS messages, geolocations, etc.).

Written reports

Written reports should be the main part of the documentation for the entire investigation, while the tool generated report should only be added as additional documentation.

Written reports, like any other, go under the general rules that are:

1. if it is not in your report, you cannot testify about it
2. your report must detail your conclusions
3. detail every test conducted, the methods and tools used, and the results.

An example of a written report is attached at the end of this workbook.

Exported files as part of the report

Files can be exported from a forensic tool and be added to the report. The evidence first needs to be introduced. Investigators need to have expectations of what could be found and what to focus on. Later on, only the files of significant evidential value that want to be additionally highlighted are put in the report – the ones that can prove or dispute the accusation.

NOTES

Questions I still have about this chapter

Ideas to discuss with colleagues

Extra notes

Further reading

While it's certainly not a written report for a specific investigation, have you ever looked at the PaCSON Annual Report (2020)? There's lots of country-specific information for you to consider, as well as regional trends – which have all been identified through reporting.

Further discussions

Have you ever considered subscribing to PILON's YouTube Channel (click here for a direct subscription link). The channel includes recordings of the class meetings from the intermediate digital forensics course (as well as last year's fundamentals cohort).

Further Resources

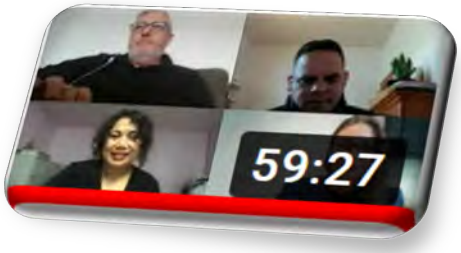
Further PILON videos

PILON recordings of zoom meeting with previous cohort

On PILON's YouTube Channel (subscribe here) we've uploaded recordings of the class meetings from last year's Fundamentals course. You might want to watch some of the videos to understand more about digital forensics in action within the Pacific.

'Digital Forensic Process' (week 4)

Week 4 of the pilot course covered the 'Digital Forensic Process'. In this video, we hear from Jon Peacock and Damian Rapira-Davies at the NZ Department of Internal Affairs



'Digital Evidence Preservation' (week 7)

Our expert speakers, Jon Peacock and Damian Rapira-Davies from the New Zealand Department of Internal Affairs again share their knowledge in this video about digital evidence preservation.

'Computer Forensics Introduction' (week 9)

Superintendent Kalisi Tohifolau and CERT representative Siosaia Vaipuna join us in this video to share their knowledge about computer forensics and provide insight into how police and the Computer Emergency Response Team work together in the Kingdom of Tonga.

'Computer Forensics Introduction' (week 10 for Lawyers)

Esther George, CEO of Zyber Global and Kresimir Hausknecht, head of the Digital Forensics Department at Insig2 speak in this video about presenting digital evidence in court. This presentation concluded the final discussion group for the pilot 'fundamentals of digital forensics' scholarship cours in 2021.

PILON recordings of zoom meeting with the intermediate level cohort

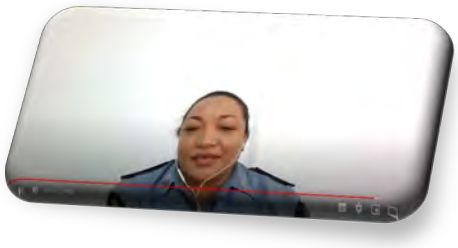
On PILON's YouTube Channel (subscribe here), we've also uploaded recordings of the class meetings from the intermediate digital forensics course (this follows on from the Fundamentals course). You might want to watch some of the videos to understand even more about digital forensics in action within the Pacific.

Topic: Digital Forensics and the New Zealand Department of Internal Affairs

This first webinar is part of a multi-part series for the Zyber/Insig2 "Digital Forensics for Lawyers and Judges - Intermediate level" scholarship course delivered by the Working Group. With thanks to our presenters from the New Zealand Department of Internal Affairs - Te Tari Taiwhenua

Topic: Digital Forensics and IT Investigation Unit with the Fiji Police Force

This second webinar is part of a multi-part series for the Zyber/Insig2 "Digital Forensics for Lawyers and Judges - Intermediate level" scholarship course delivered by the Working Group. With thanks to our presenter Corporal Savenaca Siwatibau, Digital Forensics and IT Investigation Unit, Fiji Police Force



Topic: Police & Prosecutor Perspectives on Digital Forensics

This third webinar is part of a multi-part series for the Zyber/Insig2 "Digital Forensics for Lawyers and Judges - Intermediate level" scholarship course delivered by the Working Group. With thanks to our presenters Leotrina Macomber, former Crown Counsel and Kalisi K. Tohifolau, Acting Deputy Police Commissioner

Further PILON resources

There's plenty of publicly-available resources on the PILON Cybercrime Working Group's Digital Library and more in the members zone (which you can join).

PILON resources on working with other countries on digital evidence

2020 The PILON Mutual Legal Assistance Handbook: Cybercrime & Electronic Evidence. This handbook has been developed to assist criminal justice practitioners in the Pacific to obtain, and provide, material (particularly electronic evidence) through mutual legal assistance that critical for criminal investigations and prosecutions.

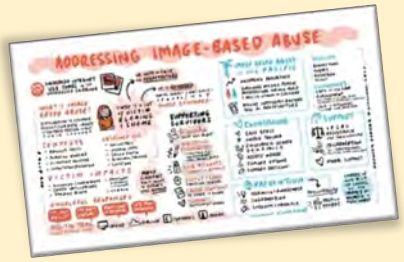
It provides an overview of cybercrime and electronic evidence, mutual legal assistance processes including specific step-by-step advice on both outgoing and incoming mutual legal assistance requests as well as helpful summary profiles of PILON members, key partner countries and popular service providers with contact information, legislative requirements and hyperlinks. You can download the full handbook here, or read the handbook online here.

2020 PILON Webinar: Mutual Legal Assistance - Electronic Evidence and Cybercrime. You can view a recording of the webinar here, or download the agenda or presentations by going to the PILON Cybercrime digital library.

2019 Cybercrime Workshop Booklet – International Cooperation to Share Electronic Evidence to Combat Cybercrime. The agenda and presentations from this workshop can be found on the Council of Europe's website. You can also download a copy of the workshop booklet here.

PILON resources on combatting online abuse

2021 Webinar series "Addressing Image-Based Abuse". To view part 1 of the webinar series click here. To view part 2 of the webinar series click here. To view the posters, go to the Cybercrime Working Group page.



2021 Cybercrime and Children in a Covid-19 World. To view the part 1 of the series on cyberbullying click here. To view part 2 of the webinar series on Online Child Abuse Material (CAM) click here. To view the posters, go to the Cybercrime Working Group page.

2018 Cybercrime Workshop Booklet – Combatting online child abuse and cyberbullying in the Pacific. You can download a copy of the workshop booklet here.

PILON resources on understanding the Pacific response to cybercrime

2020 PILON Week Webinar - The effects of COVID-19 on cybercrime in the Pacific You can view a recording of the webinar here, or download the poster or presentations by going to the PILON Cybercrime digital library.

2017 Cybercrime Workshop Booklet – The Pacific response to cybercrime: effective tools and good practices. You can download a copy of the workshop booklet here.

Solomon Islands background and self-reflections

Solomon Islands legislative profile

In the Solomon Islands, there is no stand-alone legislation or a clear guideline or direction under any law that governs the use of, or procedures or process for obtaining digital evidence, when there is a need for it to be produced in a criminal proceeding.[1]

Evidence Act 2009	At the most, section 91 of the Evidence Act 2009 allows a party to a proceeding to produce evidence, including that which is digital. Parties are allowed to produce copies of the document/evidence if it is clear that it is the only way of making that evidence available for the court and parties to view.[2] The importance of verifying and authenticating digital evidence cannot be overstated. It is the responsibility of the Prosecutor to produce this evidence on oath before the court can accept it. If it is video footage, the Prosecutor must ascertain the following:[3] • the type/brand of the machine (in this case- CCTV) • who installed the machine, and who operates it; • the person who was present when the machine recorded the footage and his experience in explaining how the machine works or how to read it; • an expert who is qualified to confirm that the representation of the piece of digital evidence relied on is accurate; or • a witness who can testify to explain how the machine works and its operation from which the digital evidence was obtained.
Police Act 2013	The Police Act 2013 enables police officers to obtain digital evidence as part of investigations and gathering evidence. The Act gives the police powers to keep such evidence in its custody for investigations and court proceedings.[4] The Office of the Director of Public Prosecutions, receives a lot of briefs from police and other stakeholders with digital evidence. The most common form of digital evidence received is that of CCTV footage and still photographs from Surveillance Cameras.

[1] Police typically apply the traditional methods in evidence gathering only. There is not much in terms of a process or procedure applicable with this type of evidence.
[2] See section 91 (1) (2) of the Evidence Act 2009 retrieved from http://www.paclii.org/sb/legis/num_act/ea200980.
[3] Chapter 8: Admissibility of Evidence, Criminal Law in Solomon Islands retrieved from http://www.paclii.org/sb/criminal-law/ch8-admissability-of-evidence.htm
[4] See sections 105 and 106 of Police Act 2013 retrieved from http://www.paclii.org/sb/legis/num_act/pa201375

ODPP Solomon Islands' consolidated digital forensics self-reflections

Self-reflection on Standard Operating Procedures

1. Police investigators should be educated on understanding, handling and preserving digital evidence. The police should formulate a simple Standard Operating Procedure (SOP) on handling digital evidence (procedure for acquisition protection and preservation). That SOP will be a guide to investigators who deal with digital evidence. It will show them the process or procedure to follow.

Self-reflection on specialised computer forensic teams

2. Police should have a specialised computer forensic team instead of engaging outside IT technicians. Their 2020 SOP should be reviewed to include digital exhibits and how to deal with them.

Self-reflection on the Evidence Act 2009

3. Our Evidence Act 2009 should be reviewed, to include detailed provisions on digital evidence.

Self-reflection on crime scene protocols

4. Police should have protocols for dealing with digital evidence at crime scenes. This is to avoid errors, oversights or damage to the evidence. The investigator responsible for securing a crime scene, whether first responders or digital evidence examiners, should be trained to follow accepted protocols. These protocols should prevent contamination or damage to evidence.

(Continued)

Self-reflection on digital evidence identification

5. After securing the crime scene, the Investigators/his superiors should identify the type of digital evidence that is required or has the potential to assist the police in solving the crime. This should include identifying, recognising, and documenting potential digital evidence at a scene. The process should identify digital storage media and processing devices that may contain evidence relevant to the police to assist them in their investigation.

Self-reflection on digital evidence handling

6. After the relevant evidence is identified, the procedure for collecting the evidence must be clearly set out. The evidence collected should be appropriately recorded and packaged before it is removed from the scene of crime.

Self-reflection on original copies

7. Investigators and prosecutors must ensure that the evidence is preserved while it is in their possession after it is acquired from the scene of crime. The original copy should never be altered. It must be preserved for production during the trial. Investigators and prosecutors should use a working copy in preparation for the trial.

Self-reflection on understanding footage

8. Prosecutors should be trained to understand the functions of a digital machine, how to read it and the process of translating it into evidence to assist the court. The Prosecutor must know how to read and understand the footage's timing, and sequence before trial. If using Digital evidence to illustrate the theory of the case, it must align with the footage's sequence and timing.

Consolidated CDPP tips

Judy King (Principal Federal Prosecutor)
Jon Emmet (Principal Federal Prosecutor)

Continuity and integrity of the data:

1. If challenged, prosecutors must be able to prove that the device or digital evidence presented in Court is the same as the device or digital evidence seized during the investigation.
2. To assist in doing so, prosecutors should prepare a table for themselves, and potentially the Court if accepted, that summarises each step in the chain of custody, including, for example, the seizing officer, any other police officer involved in handling the evidence at the time of seizure, and how the device was stored.
3. Prosecutors must be in a position to demonstrate that the device was not interfered with while it was in storage, which might have affected the integrity of the data. For example, prosecutors may need to play to the Court the full video examination by police of the device, or tender evidence of property seizure records or exhibit custody records.

Assessing admissibility:

1. Prosecutors must be ready to identify how the piece of evidence is admissible, starting first with why it is relevant to the prosecution case. Digital evidence may be relevant for multiple reasons, including (but not limited to) online communications that are admissions, records found on a device that prove the identity of a defendant, or the defendant used an online system (such as social media or online storage) as part of committing the alleged offence. Digital evidence may also be relevant because it proves a negative, for example that no record existed.
2. Identifying that a piece of evidence is relevant is not enough, prosecutors must also understand the basis on which the evidence is admissible. The evidence may be direct evidence (for example, the fact a device was located in a defendant's bedroom), or it may be circumstantial evidence (for example, photos found on a defendant's phone).
3. In assessing admissibility, depending on the evidence, prosecutors must consider whether the piece of evidence is relied on as a document/record or real evidence, whether the piece of evidence is being used for a hearsay purpose, and what the relevant hearsay exception is.

Expert evidence:

1. Digital evidence can vary in its complexity, depending on its content and how the prosecutor is seeking to use the evidence. Some evidence may only be admissible if it is produced by an expert who can give an opinion of specialised knowledge based on the person's training, study or experience. For example, a police officer may be able to give evidence about text messages located on specific device, but is unlikely to have sufficient expertise to give evidence about how metadata can be altered on a device,
2. Prosecutors must ensure any proposed expert has sufficient expertise to give evidence about the specific issue, and that their evidence does not go beyond their expert knowledge.
3. It is recommended that prosecutors should engage early with informants about the terms of any expert briefing to ensure that relevant and admissible opinion evidence is secured.
4. Prosecutors must also be alert to defendants or their lawyers purporting to give evidence or opinions on technical concepts about which they are not experts.

Assessing weight:

1. It is a common misconception that circumstantial evidence is somehow inherently of less weight than other sorts of evidence. In reality, most cases mostly involve circumstantial evidence, in particular, any inference of what was in a defendant's mind is almost invariably a matter of circumstantial evidence.
2. Circumstantial evidence is strengthened by assessing it in the context of the overall prosecution case, including considering other pieces of circumstantial evidence. Often a device will contain large amounts of data and metadata that a prosecutor can rely on to strengthen the evidence. For example, in most cases, a prosecutor can rely on the metadata of specific photograph, which may show the date and time it was taken, the location it was taken, and the device used to take it.

Proving ownership or use of a device:

1. Often, key evidence may be located on a device, but there is a question about whether a defendant the defendant owned or was the user of that specific device. For example, if a phone is located in a house in which multiple people live, the Prosecutor must establish that the defendant was the person who sent/received the relevant messages/calls, or took the relevant photographs.
2. To do this, prosecutors can rely on a number of other pieces of evidence, such as where the device was located (for example, was it seized from the defendant's bedroom), the content of social messages (for example,

messages between a defendant and a family member which refer to the defendant by name), and the content of photographs (for example, "selfies" of the defendant being taken on the phone).

Presenting evidence

1. Prosecutors can present digital evidence in a variety of ways, depending on its complexity, purpose and ease of access.
2. The simplest way to present individual and self-explanatory evidence is by taking photographs of the device or using screen shots. For example, if the evidence is a series of text messages between two defendants, prosecutors can present this by printing a series of screenshots of the conversation. Where this is done, it is important to ensure that dates and times are also captured.
3. Where the digital evidence is voluminous, prosecutors might prepare a summary table to assist the Court. For example, if a particular phone contains a large amount of evidence relevant to the Crown case, a prosecutor can prepare a table summarising thing like the serial number, make and model, profile information, contacts, text messages, and photographs taken.
4. If the evidence is more complex, such as technical evidence about how files are saved, prosecutors might ask the relevant witness to prepare explanatory charts to give a visual representation to the Court to aid in understanding.
5. Prosecutors should consider how they will communicate technical concepts to the Court, and anticipate areas that the judge may find challenging. For example, some judges are unlikely to have used social media services such as Facebook, and therefore prosecutors should be prepared to explain simple concepts such as the "feed", a person's "wall", "friend requests", and "tagging a friend" in a photo. This may be evidence that the prosecutor needs to lead through a witness, such as the investigating officer or complainant.

Sensitive evidence

1. Prosecutors should be mindful to ensure that sensitive evidence is quarantined and not disclosed in a brief of evidence. Examples of sensitive evidence includes child abuse material (textual, videos and photos) or offensive material.
2. Prosecutors should make such material available to defence representatives for inspection to ensure that there is full and proper disclosure, to guarantee a defendant's right to a fair trial.

Procedural examples

Digital forensics examination notes

CASE DETAILS			
CRB No:		Forensic Case No:	
Location of Examination:			

HANDOVER		
Photos: ☐ Yes ☐ No	Power Cords: ☐ Yes ☐ No PIN No: ☐ Yes ☐ No A power cord and PIN numbers (SIM and Handset) MUST be provided by the Case Officer. If not, please obtain prior to commencing examination	Item Sealed: ☐ Yes ☐ No

Description of items: _____

Item Received From

Name: _____

Date: _____ Time: _____

ITEM OPENED / SEAL BROKEN

Date: _____ Time: _____

Photographs: _____

Description _____

Components: ☐ Mobile Phone / PDA ☐ SIM / USIM Card ☐ Digital Storage Device

EXAMINATION COMMENCED

Date: Time:

EXAMINATION CONCLUDED

Date: Time:

ITEMS RE-SEALED

Date: Time:

Forensic Examiner: _____ (Signat _____

ITEMS RETURNED TO

Name:

Date: Time:

SIM 1

Brand: Condition:

Number Printed on Card: PIN Req: ☐ Yes ☐ No PIN No:

Electronic ICCID: PUK Req: ☐ Yes ☐ No PUK No:

Electronic IMSI:

Examination Method: Software Version:

Examination Notes:

SIM Cloned: ☐ Yes ☐ No

File Name: Results Copied To:

Date: Time:

SIM 2

Brand: Condition:

Number Printed on Card: PIN Req: ☐ Yes ☐ No PIN No:

Electronic ICCID: PUK Req: ☐ Yes ☐ No PUK No:

Electronic IMSI:

Examination Method: Software Version:

Examination Notes:

SIM Cloned: ☐ Yes ☐ No

File Name: Results Copied To:

Date: Time:

ADDITIONAL NOTES:

DIGITAL STORAGE DEVICE

(USB, MEMORY CARD, HDD)

Brand: _____ Model: _____

Colour: _____ Capacity: _____

Serial Number: _____ Previewed: ☐ Yes ☐ No Copied: ☐ Yes ☐ No

Photographs: ☐ Yes ☐ No

Condition: _____

Examination Method: _____ Software Version: _____

Examination Notes: _____

File Name: _____ Results Copied To: _____

Date: _____ Time: _____

MOBILE PHONE / PDA

Brand: _____ Model: _____

Colour: _____ Capacity: _____

IMEI: _____ Locked: ☐ Yes ☐ No PIN No: _____

Other ID: _____ Received: ☐ On ☐ Off Photographs: ☐ Yes ☐ No

Condition: _____

Examined With: _____ Date / Time Check: ☐ Yes ☐ No Reference Source: _____

Reference Date: _____ Reference Time: _____ Result of * # 0 6 #: _____

Device Date: _____ Device Time: _____ IMEI Verified: ☐ Yes ☐ No

Examination Method: _____ Software Version: _____

Examination Notes: _____

Forensic Examiner: _____ (Signature) Date: _____

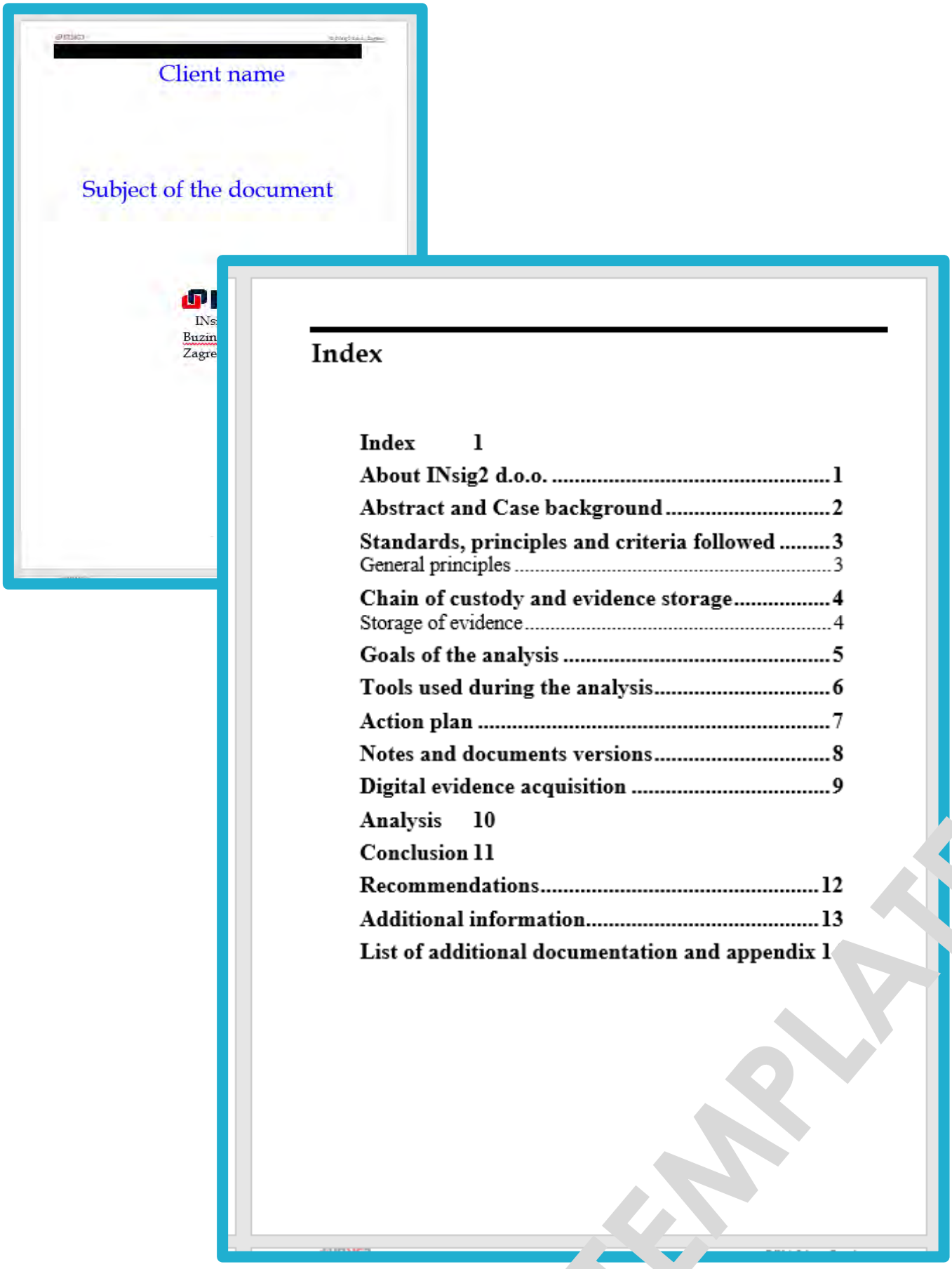
File Name:		Results Copied To:	
Date:		Time:	

ADDITIONAL NOTES:

ADDITIONAL NOTES:

Forensic Examiner: _____ (Signa _____

Example of a written report



Client name

Subject of the document

INs
Buzin
Zagre

Index

TEMPLATE

About INsig2 d.o.o.

INsig2, based in Zagreb, is a Croatian company founded in 2004, with the main focus on digital forensics. Since the first day of business activity, INsig2 has been working with digital evidence and digital forensics. It was then that we recognized digital forensics as an emerging discipline that will be impossible to avoid in any serious investigation, regardless of the type of criminal offence.

As communication between people is becoming more and more digital and as organizations' information systems hold more and more valuable and sensitive data, digital forensic discipline is impossible to avoid in any serious investigation. Police investigators involved for example in organized crime investigations, economic crimes investigation or fighting against child pornography should be very skilled in understanding principles of

digital forensic investigations. Same is true also for tax and customs authorities and competition agencies fighting against fraud, cartels and other forms of economic crime.

Since 2008, INsig2 has its own educational centre capable of conducting wide variety of forensic courses. INsig2 experts have been involved in long term cooperation with law enforcement officers from this region and has become the region leading company for providing service of digital forensic investigations. Besides the regional activity, INSig2 is also has global presence with successful project in whole Europe, middle east countries and Asia.

INsig2 continuously invests significant resources in training of its own experts and have been recognized as a reliable partner that can be relied on.

INsig2 has established partnerships with some of the most popular and globally recognized digital forensics software vendors,

which enables us to provide specific vendor trainings. Therefore, education services are becoming one of the key segments of professional services INsig2 provides in the area of digital forensics to a number of customers in the region.

Besides providing forensic training services, INsig2 has extensive experience in designing, equipping and setting up digital forensics laboratories for different government agencies and the police. In order to provide digital forensics investigators and analysts with the best working environment that perfectly suits their needs, INsig2 experts will, in line with the client's budget and requirements, suggest the best possible solution, deliver and set up all the equipment and software that any forensics expert might need when applying the most advanced solutions in the field of digital forensics. INsig2 experts will also prepare the project documentation and all relevant technical documentation in accordance with current legislation and latest standards necessary for the

optimal performance, operation and fulfilment of requirements and rules of the profession. Furthermore, INsig2 will also prepare instructions on equipment usage and maintenance.

INsig2 consultants in the department of digital forensics have many world renowned certificates that prove their competencies in various fields of digital forensics and incident response such as: CFCE, ACE, EnCE, ILO, CCPA, XRY, XWays, MCFE and many more that are available for review if necessary.

Abstract and Case background

Case introduction notes:

- Everything about the case
- Timeline of events
- Short description of the goals
- Who is the client and short history related to the case
- Events that lead up to the case
- Engagement notes
- Information received

6

Standards, principles and criteria followed

The following standards, principles, and criteria outlined below are followed in every investigation. Below we have general principles as outlined by the forensic community, principles and procedures outlined by the NIJ, and criteria recommended by the SWGDE

7

General principles

The forensic community has outlined the following four main principles to applied during investigation:

- No actions to change original data
- Investigator(s) are competent to access original data
- Audit trail created
- Legal principles are adhered to (Keener, 2017)

8

Chain of custody and evidence storage

The forensic community outlines the following areas for maintain the chain of custody:

- Name & contac nfo nation of custodian
- Detailed ide ificati n of evidence (model/ rial)
- When, hom evidence was acq or moved
- here ev ence is stored
- Wh /if eturned

9

Storage of evidence

Items are placed in a heavy-duty mechanical evidence locker room. Fingerprint security system into the room allows that both deposit and retrieval can only be performed by pre-authorized individuals whose prints have already been entered into the system. Lockers are divided into readily identifiable compartments, which are opened and closed with the user-friendly button locks. A heavy-duty steel structure, with welding at the ends to reinforce the strength of the doors. The

10

doors themselves incorporate robust load-bearing hinges and rubber stops to ensure smooth closure. The digital lockers are also enhanced with detection sensors and LED panels that display valuable information at a glance.

11

Goals of the analysis

- What are the analysis goals
- Points to prove
- What are the client requests
- What needs to be proven, disproven, checked, verified…

12

Tools used during the analysis

State all the tools that were used for this investigation, their versions and everything that needs to be noted to give analysis more weight

All hardware and software i… to be stated

13

Action plan

Steps of the whole investigation form initial interview, acquisition of data and full dana analysis steps

14

Notes and documents versions

Dates and notes of what was done

Dates of this document modifications, who performed them and what was done

15

Digital evidence acquisition

Numbered and stated all evidence sources with accompanied pictures of all steps

- Evidence source
- Type of evidence – laptop, computer, server
- How was it acquired
- Sizes, serial numbers, general data contained

16

Analysis

This part of the document will contain all details and description of work done related to the Goals of the analysis.

Everything that was found, will be explained in detail s[illegible] in case there is a need for re[illegible] or repetition of the st[illegible]s, one [illegible] easily follow the st[illegible]s and should come to the same conclusions.

During the anal[illegible]s, conclusion will be s[illegible]ted in ac[illegible]ordance with the g[illegible]ls o[illegible]e [illegible]alysis.

17

Conclusion

This is executive summary of the whole document. It will in short describe the steps taken, goals of the analysis and in easy wording state what can be concluded.

18

Recommendations

If the case required some recommendation to be stated in order to:

- Prevent the incident form happening again
- Procurement of specific software
- Implementation of security measures
- Actions need to be taken in conjunction to the case goals

19

Additional information

Report made by:

Report was delivered on the:

INsig2 d.o.o.
Buzinska cesta 58, 10010
Zagreb, Hrvatska

Signature of the examiner that created the report:

_____

20

List of additional documentation and appendix

- Documentation received form the client
- Tool generated reports
- Tool generated documents
- Important case related documents, pictures, general evidence

21

Consolidated Glossary

Allocated Data	data residing on their reserved space on a hard drive
Arson Can	a clean, empty paint can which can be found in hardware or home improvement stores
Bitcoin	a digital or virtual currency created in 2009 that uses peer-to-peer technology to facilitate instant payments
Blu-ray Disc	a disc which contains 25 GB per layer. Blu-ray is similar to normal DVD or CD in size dimension but in space, and memory is larger than DVD.
Brute Force	a type of attack on users' passwords; consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly
Camcorder	portable device used for video capture and recording
CCTV (Closed Circuit Television)	also known as video surveillance; is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors
CDMA (Code-Division Multiple Access)	a mobile phone service technology which is, opposed to GSM, primarily used in the United States of America and parts of Asia by other carriers
Chain of Custody	the forensic link, the paper trail, or the chronological documentation of electronic evidence which indicates the collection, sequence of control, transfer, and analysis
Child Abuse Material (CAM)	the term unifies a collection of illegal pictures/videos of underaged children
Cloud	a general term for anything that involves delivering services over the Internet
Cluster	a group of sections (the smallest unit that can be accessed on a storage device, like an HDD or SSD) that make up the smallest unit of disk allocation for a file within a file system. In other words, a file system's cluster size is the smallest amount of space a file can take up on a computer.
Computers & Laptops	electronic devices for storing and processing data according to instructions given by the user
CPU (Central Processing Unit)	the main processor within a computer that executes instructions that make up a computer program
Cryptocurrency	related evidence is a digital asset, like money. There are hundreds of different cryptocurrencies on the market, the most popular one being Bitcoin. For investigators, the most important evidence to find is a so-called, cryptocurrency wallet. A cryptocurrency wallet is a software program that stores private and public keys that enable users to send and receive digital currency
Cryptographic Key	a string of data that is used to lock or unlock cryptographic functions, including authentication, authorisation, and encryption
Cryptography	the study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents
Digital Versatile Disc or Digital Video Disc (DVD)	a digital optical disc storage format used to store high capacity data, like high- quality videos and movies.

Digital Video Recording Systems	devices that record video in a digital format to disk drives, USB flash drives, SD memory cards or other storage devices
Email Address	identifies an email box to which email messages are delivered. It is made up of a local-part (e.g. john.smith), an @ symbol, and domain (e.g. gmail.com)
Environmental Control	the extent to which there is a forensically sound examination environment (a working environment that is completely under the control of the forensic examiner at all times)
External Devices	devices which are physically not a part of the computer but can be plugged in, and data can be transferred to or from them and transmitted to another computer They are crucial to be acquired in an investigation as digital evidence is often stored on them.
Faraday Bag	a bag made of a special material that blocks electromagnetic signals. It is used to hold devices, such as mobile phones, in order to repel outside signals from interfering with the contents of the device
FAT (File Allocation Table)	a file system developed for hard drives that originally used 12 or 16 bits for each cluster entry into the file allocation table. It is often found in flash memory, digital cameras, and portable storage devices
FDE (Full Disk Encryption)	the encryption of all data on a disk drive, including the program that encrypts the bootable Operating System (OS) partition
Fraud	wrongful or criminal deception intended to result in financial or personal gain
Gaming Consoles	can be used for communicating with other players and can connect to the Internet. They are prone to similar forms of misuse and abuse as personal computers
GSM (Global System for Mobile Communications	a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets
Hashing	the process of transforming any given key or a string of characters into another value
Home Intelligent Personal Assistant	a software agent that can perform tasks or services for an individual – based on commands or questions. Some virtual assistants can interpret human speech and respond via synthesised voices
Identity Theft	the fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc
Imaging	the process of creating a forensic copy or image
In-Vehicle Infotainment Systems/Navigation Systems/GPS Devices	the systems in vehicles which can often provide historical data to show where a vehicle was at specific times, areas frequently visited, new locations travelled, future planned locations, and how long a vehicle was at a particular location
IoT (Internet of Things) Devices	a relatively new area in information technology. IoT device is a piece of hardware that transmits data from one place to another over the Internet
ISO Certification	a set of standards (published by the International Organization for Standardization or ISO) that help organisations ensure they meet particular standards (including regulatory requirements) related to that product or service. The ISO certification is a written assurance that the product, service or system in question meets specific requirements.
Journaling File System	a file system that keeps track of changes not yet committed to the file system's main part by recording the intentions of such changes in a data structure known as a "journal". Such files can be helpful in case of a

	system crash or power failure as they can be brought back online more quickly with a lower chance of being corrupted
LAN (Local Area Network)	a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building
Logs	files that record either events that occur in an operating system or other software runs or messages between different users of communication software
Malicious Hacking	the gaining of unauthorised access to data in a system or computer in order to perform malicious activities which intention is to harm the data or system
Malware (Malicious Software)	any software that is intentionally designed to cause damage to a computer, server, client, or computer network. The most common types of malware are viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware
MBR (Master Boot Record)	the most important file of the FAT files system; holds information on how the logical partitions, containing file systems, are organized on the medium.
Metadata	files containing data that provide information about other data – "data about data
MFT (Master File Table)	a file in which information about every file and dictionary of an NFTS file system is stored
Mobile Devices & Tablets	any devices running a mobile operating system (such as mobile phones, smart home appliances, smart cars, etc.)
Network Devices (routers, HUBs, etc.)	electronic devices which are required for communication and interaction between devices on a computer network. Investigation of network devices is part of network forensics
NTFS (New Technology File System)	a file system first introduced by Microsoft in 1993. It is the most common file system for the end-user computers based on Windows operating systems
Partition	a section of the hard drive that is separated from other segments. Having multiple partitions enables users to divide a physical disk into logical sections (e.g. allowing multiple operating systems to run on the same device)
Plagiarism	the practice of taking someone else's work or ideas and passing them off as one's own
RAM (Random Access Memory	a form of computer memory, typically used to store working data and machine code. It is considered volatile, as it requires power for the data to remain accessible
Ransomware	a type of malicious software designed to block received, decoded and displayed on a television
Set-Top Box	a device that allows a digital signal to be received, decoded and displayed on a television
Slack Space	the storage area of a hard drive ranging from the end of a stored file to the end of that file cluster.
Smart Appliances	used together to enable the concept of a smart environment. Such data contain valuable forensic information about events and actions occurring within a smart environment and, if analysed, can help breach security policies
Smart Home Automation	controls lighting, air conditioning, entertainment systems, and appliances. It may also include home security such as access controls and alarm systems. When connected to the Internet, home appliances are an important component of the Internet of Things
Solid State Disks (SSD)	store data with the use of flash-memory chips (called NAND flash memory).

Sterile Media or Sterilisation	magnetic media on which every byte has been overwritten in order to eliminate any data that previously existed on the media. The process of achieving this is also called “wiping” or “sterilising”.
Unallocated Data	data residing in ‘free’ space on the disk after being deleted. Unallocated space is available to store new data even though it may contain old data which would then be overwritten by new data
Unmanned Aircraft Systems (Drones)	remote-controlled pilotless aircraft or small flying devices which store data in digital formats, which have become a tool for criminal activities (causing drone forensics to become a new and important part of digital forensics)
Unstructured Data	information that either does not have a pre- defined data model or is not organised in a pre-defined manner
USB Flash Drive	a device used for data storage that includes a flash memory and an integrated Universal Serial Bus (USB) interface.
URL (Uniform Resource Locator)	a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. In web browsers, URLs are mostly displayed above the page in an address bar
Validation	the process of verifying that something works as it is expected to work
Volatile (Flash) Memory	memory storing data that gets lost when the computer is turned off
Virtual Private Network (or VPN)	an application installed on a device that redirects your internet connection through its own servers around the world, allowing the user to virtually change their location online, making them more anonymous
Wangiri Fraud	refers to the activity of calling a victim’s mobile phone and hanging up after one ring, hoping the victim will return the missed call out of curiosity or courtesy. If the victim does, he or she unsuspectingly calls an expensive premium number
Wearable Technology or Wearables	smart electronic devices that can be incorporated into clothing or worn on the body as accessories. Wearables include activity trackers, smartwatches, body cameras for law enforcement, wearable technology for assisted living, and fashion electronics
Wiping or Sterilising	the process of unrecoverable deleting all the data from a digital evidence

Level 6, TATTE Building
Sogi, Apia
SAMOA
www.pilonsec.org
pilon@pilonsec.org

Buzinska cesta 58,
10010 Zagreb,
CROATIA
www.insig2.com
info@insig2.com

Zyber Global Centre
High St Herne Bay, Kent CT6 5NP
UNITED KINGDOM
www.zyberglobal.com/
office@zyberglobal.com