CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Christian Braccini, Teemu Väisänen, Michal Sadloň, Hayretdin Bahşi, Agostino Panico, Kris van der Meij, Mario Huis in 't veld

BATTLEFIELD DIGITAL FORENSICS

DIGITAL INTELLIGENCE AND EVIDENCE COLLECTION IN SPECIAL OPERATIONS

Tallinn 2016

www.ccdcoe.org
publications@ccdcoe.org

About the NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the USA as Sponsoring Nations, and by Austria and Finland as Contributing Participants. The Centre is not part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information-sharing between NATO, NATO member states, and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

Foreword

Troops in contact in the battlefield are very likely to be exposed to the enemy's digital information.

Digital media collection by Special Operation Forces (SOF) might provide the critical information needed to penetrate the enemy's decision matrix and support legal actions against insurgents.

Following up on Dr William G Perry's ideas for 'Assuring Digital Intelligence Collection' [1], this publication presents a set of tactical techniques for SOF forensics teams to maximize the effectiveness of digital data collection while running combat-compressed operations. The latest technical research findings in terms of digital forensics techniques, anti-forensics measures and acquisition network architectures are considered.

As exploitation of digital information in the battlefield can lead to a strategic payoff, proper electronic evidence collection is one of the biggest challenges for SOF, particularly given the chaos and unpredictability in the battlefield. With the evolution of technology, SOF operators are, however, expected to perform increasingly advanced core activities on-site

This study provides guidance for prioritisation in the ray of force protection, the primary consideration for responders. Their challenge is creating rapid and automated techniques that aim to prioritise collection while establishing a chain of custody. By analysing the tactical requirement and merging it with the available technologies, the authors propose a structured approach toward digital intelligence and evidence collection, in combat compressed operations. From the constraints of combat operations in a hostile environment, different techniques might be adopted and tailored to potentially less restrictive settings ranging from foreign internal defence to counter-terrorism missions where the digital data represent a major payoff.

The project is the joint effort of the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Technical University, "La Sapienza" University (Rome) and Military Police Centre of Excellence (Bydgoszcz).

Christian Braccini

Table of Contents

Figures

Table

Flowcharts

1 Glossary

ABSOLUTE	Aerial Base Station with Opportunistic Links for Unattended and Temporary Events
AeNB	Aerial eNodeB, used in ABSOLUTE
BIoT	Battlefield Internet of Things. The set of IT devices, the information processed and the opposing force making use of them in the battlefield
binary	Technique for representing data as a series of 1s and 0s
C2	Command and Control
CCIR	Commander's critical information requirement
CD	Compact Disk
CELLEX	Cell-phone exploitation
CPU	Central Processing Unit. Portion of the computer where high-speed computations occur
COP	Common Operational Picture. A single identical display of relevant information shared by more than one command
computer forensics	Application of computer investigation and analysis techniques to determine potential legal evidence (or intelligence)
data	Representation of facts that can be used for processing and creating information for decision-making
DF	Digital forensics
DFA	Digital forensics asset
digital evidence	Information that is stored or transmitted in electronic format using the binary numbering system
DMA	Direct memory access
dongle	A device that plugs into an available computer port (USB) and performs a useful service such as encryption, infrared data transfer, or network connectivity)
DTN	Delay-tolerant networking
DVD	Digital versatile disk (or digital video disk)
evBO	Evidence-based operations
FP	Force protection
FOB	Forward Operating Base. In special operations, a base usually located in friendly territory or afloat that is established to extend command and control.
GUI	Graphical user interface
hardware	Any object or component that can be associated with a computer system
HDD	Hard disk drive
HID	Human interface device, commonly refers to USB HID class devices (keyboards, mice, or game controllers)
ICC	International Criminal Court
information	Processed data
information assurance	Methods and techniques used to assure the confidentiality, legacy, integrity and nonrepudiation of information
information operations (IO)	Integrated employment of the core capabilities of electronic warfare, computer network operations, psychological, deception, and operations security.
Internet	Network(s) that connects millions of computers across the globe using internationally accepted protocols
Intsum	Intelligence summary
IP	Internet protocol. The standard that works with the transmission control protocol (TCP)—that is, describes how an internet-connected computer should break data down into packets for transmission across the network, and how these packets should be addressed so that they arrive at their destination.
IT	Information technology
ITTI	(IT)Target Infrastructure (ITTI)
Laptop	A portable computer.

LED	Light-emitting diode assembled into various types of lamps
Linux	Computer operating system
LTE	Long-term evolution, commonly known also as 4G LTE.
MANET	Mobile ad hoc network, a self-configuring, infrastructure-less network of mobile wireless devices.
materiel	The equipment, apparatus, and supplies of a military force. It can apply to weapons, aircraft, parts, support equipment, ships, and almost any other type of equipment used by the military.
MEDEX	Media exploitation
media	Computer storage mechanisms (such as hard drives, SSD disks, USB flash drives, CD/DVD disks, or SD cards)
NAS	Network-attached storage
OPSEC	Operational security. Prevention of plans, troop numbers and strategy from getting to enemy
OS	Operating system
PDA	Personal digital assistant, a small device that can include computing, telephone, paging, networking, and other features
PLMU	Portable land mobile unit, a standalone and self-sufficient communication platform
RAID	Redundant array of independent disk
RAM	Random-access memory
RFID	Radio-frequency identification
RJ45	Registered jack 45, a connector type meaning actually generic 8 position 8 contact (8P8C) modular connector.
ROM	Read-only memory, type of non-volatile memory
SD	Secure Digital, a non-volatile memory card format
SOF	Special Operation Forces. Military units that are highly trained and use special equipment, weapons and tactics, including battlefield digital forensics
SOF(DFA)	Special Operation Forces Digital Forensics Asset
strike	Action to achieve the advantages of speed, surprise, and violence against an unsuspecting target.
SSD	Solid-state drive (or solid-state disk)
tag	Refers to small wireless tags attached to devices, using Bluetooth or other wireless technologies to locate the devices or alert the owner if they have been dropped, forgotten or stolen
TEO	Technical exploitation operation
TO	Theatre of operations, a sub-area in a theatre of war defined by the geographic combatant commander required to conduct or support specific combat operations. Usually referred to as ‘theatre’.
TOC	Tactical Operations Centre
TSE	Tactical site exploitation
TTP	Techniques tactics procedure
TQ	Tactical questioning
USB	Universal Serial Bus, standardized connection type of computer peripherals
WiMAX	Worldwide interoperability for microwave access. A family of wireless communications standards designed to provide high data rates or long-distance communication.
WLAN	Wireless local area network
WSN	Wireless sensor network
QoS	Quality of service

2 Introduction

Christian Braccini

2.1 The Battlefield Internet of Things

The enemy, whether an insurgent or a conventional, symmetrical one, needs to communicate. Command and Control (C2) structures supporting the enemy's operations reflect the technological evolution; and this particularly applies to the miniaturisation of components providing the always-connected modality (Internet of Things) in the battlefield. Digital data are therefore present in the form of devices associated with cyber-personas, being used in coordinating military or insurrectional activities. These activities may consist of financing dormant troops or recruiting and training terrorists to operate in the coalition's homelands. In this regard, digital data collected from the battlefield, as evidence, might prove of strategical importance in dismantling the enemy's network. The *'Battlefield Internet of Things'* (BIoT), including the systems that insurgents use and the information they process over the internet via smartphones, computers, tablets, PDAs, etc., must be successfully exploited: digital intelligence collection is an opportunity that coalition forces cannot allow to pass by.

2.2 Exploitation of Digital Data

The battlefield is characterised by the extensive use of digital devices to process information. The capability to exploit digital data, either in the form of *media exploitation* (MEDEX) or *cell-phone exploitation* (CELLEX), has assumed a fundamental role in providing *actionable intelligence*, denying the enemy resources, or securing a criminal conviction. In the intelligence cycle, digital elements of information collected from targeted sites, once technically exploited, are disseminated in the form of intel-warnings on hostile activities. Friendly forces can therefore maintain up-to-date situational awareness by feeding into their Common Operational Picture (COP).

From an intelligence exploitation perspective, digital data differ considerably from paper documents and cannot be handled in the same way. The science of digital forensics, aimed at covering this gap, is still in its infancy, with standards and best practices struggling to keep up with the lightning introduction of new technologies. Digital forensics does not only relate to laptop and desktop computers: it includes mobile devices, networks and cloud systems. It may also include the analysis of logs, passwords and internet access, decoding data hidden with steganography, or retrieving deleted data from unallocated space, in order to build a virtual user profile during an investigation.

The work of *crime scene investigation*, more mature compared to battlefield forensics, has also benefited considerably from the introduction of digital forensics techniques. Digital data collected from the scene are volatile in nature due to the complexity of their structure (file, database, information) and the fragility of digital storage devices. Incorrect handling of devices may result in consistent data loss. Anti-forensics techniques are significantly exploiting these vulnerabilities. Digital evidence collection needs to ensure that no alteration has occurred, from the very beginning of the chain of custody, in order to maintain its probative value.

Crime scene investigation differs in many aspects from the battlefield environment, where other factors such as force protection, agility and rapidity have predominant roles. This applies particularly to Special Operation Forces (SOF), whose characteristic Technical Exploitation Operations (TEO) produce extra complexity but considerable intel-payoff in terms of digital evidence collection.

The set of recommendations that this paper provides is intended to assist Special Forces or any other first responders in recognising, collecting and safeguarding digital evidence in a hostile environment, most likely in a TEO contest. It is not all-inclusive, but addresses situations encountered in combat-compressed operations where exposure to enemy Information Technology (IT) systems occurs. When digital media devices can be

properly discovered, preserved and assured, they can be further exploited for intelligence and legal purposes. The paper, ideally a continuation of William G. Perry's study [1] focuses on the digital forensics triaging methodology to be applied during any digital intelligence collection on the battlefield. It further expands Perry's proposed approach by addressing the latest digital challenges and opportunities that first responders are likely to face in conducting their missions. Nonetheless, each operation is unique: mission critical factors, available technology and first responders' judgment should all be taken into account.

.

3 Statement of the Problem

Christian Braccini

3.1 Digital Intelligence and Evidence Collection

Today's military is adapting to asymmetrical warfare and evolving real-time threat matrices that require new approaches to military operations. Digital intelligence and evidence collection (as part of *site exploitation*) represent the new approach in targeting mobile, social, virtual and collaborative threat models to process information.

Site exploitation is composed of *tactical exploitation* and *technical exploitation* as described in ATP 3-90.15 [2].

Tactical site exploitation consists of activities performed at or near a specific spot. These activities enable materiel at the site to be effectively detected, collected, and processed. The materiel exploitation that follows will likely answer information requirements and facilitate future operations.

Conversely, technical exploitation is conducted off-site, in most cases. The security environment of forward operating bases (FOB) or national-level laboratories for technical exploitation allows for the later use of advanced processing techniques.

ATP 3-90.15 [2] further describes the use of forensic-based procedures to ensure that identification and collection tasks support the analysis and dissemination in the targeting cycle presented in Figure 1. The targeting cycle can quickly take apart the network of an insurgency or at least damage it to such an extent as to make it a low-level threat.

Figure 1. The Targeting Cycle [3].

As tactical site exploitation capabilities evolve, Special Operations Forces (SOF) are challenged with more technically advanced core activities on-site, including:

- Search techniques;
- Biometrics;
- Forensics; and
- Document and media exploitation.

From a targeting perspective, digital media found in a site potentially produce evidence indicating C2 activities with nodes of the enemy's network (proxies). A thorough Tactical Questioning (TQ) of detainees might provide hints for the attribution of social media accounts operating C2 covert activities. A surveillance operation of proxies' location potentially produces further intelligence and a subsequent raid, which in turn provides other evidence and more intelligence.

Site exploitation is composed of five core activities [2]:

- Detect;
- Collect;
- Process;
- Analyse; and
- Disseminate.

These activities inform the methodology (triage) to adopt during the media and cell-phone collection performed while on site, which is of specific interest in this paper. A dedicated paragraph will address the (digital) triage in the context of site exploitation compressed operations.

3.2 The SOF Digital Challenge

The likelihood that SOF will encounter enemy computers, portable electronic equipment and digital storage media has definitely grown since Perry [1] first stated it. One of the biggest challenges for SOF is collecting and handling the discovered data so that it can be subjected to forensic analysis. As Perry [1] explains, 'successfully discovering, preserving, and assuring digital intelligence for exploitation and legal purposes is essential to support mission assurance and national security objectives'. Digital data are inherently volatile due to the complexity of their structure and the fragility of the digital storage; the corruption of a few bits of data might render the information impossible to retrieve. In order not to contravene courts' rules of admissibility, digital-based evidence has to be presented in a suitable way that will lead to the successful conviction of terrorists.

How can SOF conduct tactical site exploitation (from tactical entry, discovery of digital assets and the establishment of a valid chain of custody) without endangering the lives of operators, while still assuring the integrity of digital information?

When dealing with digital evidence, general forensics procedures should be applied:

- The process of collecting, securing, and transporting digital evidence should not alter the evidence.
- Digital evidence should be processed only by those qualified specifically for that purpose.
- Everything done during the seizure, transportation and storage of digital evidence should be fully documented, preserved and available for review.

Chaos and unpredictability characterise the battlefield. Force protection (FP) and prioritisation should remain the primary consideration for responders. Assuring electronic evidence collection is therefore one of the biggest challenges for SOF. Every team operating on the site will have to rapidly identify sources of valuable digital information, document the findings, and secure computers and storage media. To accomplish this new mission, SOF will consider employing a Digital Forensics Asset (DFA), 'which basically is adding yet another skill to SOF's already full rucksacks' [1].

4 The SIDSS Triage

Christian Braccini

In [1] Perry has identified a set of 'rational and well-conceived principles to guide operators when involved in the search and seizure of digital information and electronic devices'. The set, underpinning the *scan, identify, document* and *secure* phases of the process, is further expanded with the sustain phase in this monograph. Basic principles are as follows:

1. **SCAN**
    a. Visually scan the environment for the presence of electronic media and devices. Be aware of hidden and obfuscated devices.
    b. Scan the area for the presence of a wireless/wired network. Use the information obtained to calculate the probable number of devices. However, be aware that fake networks may also exist.

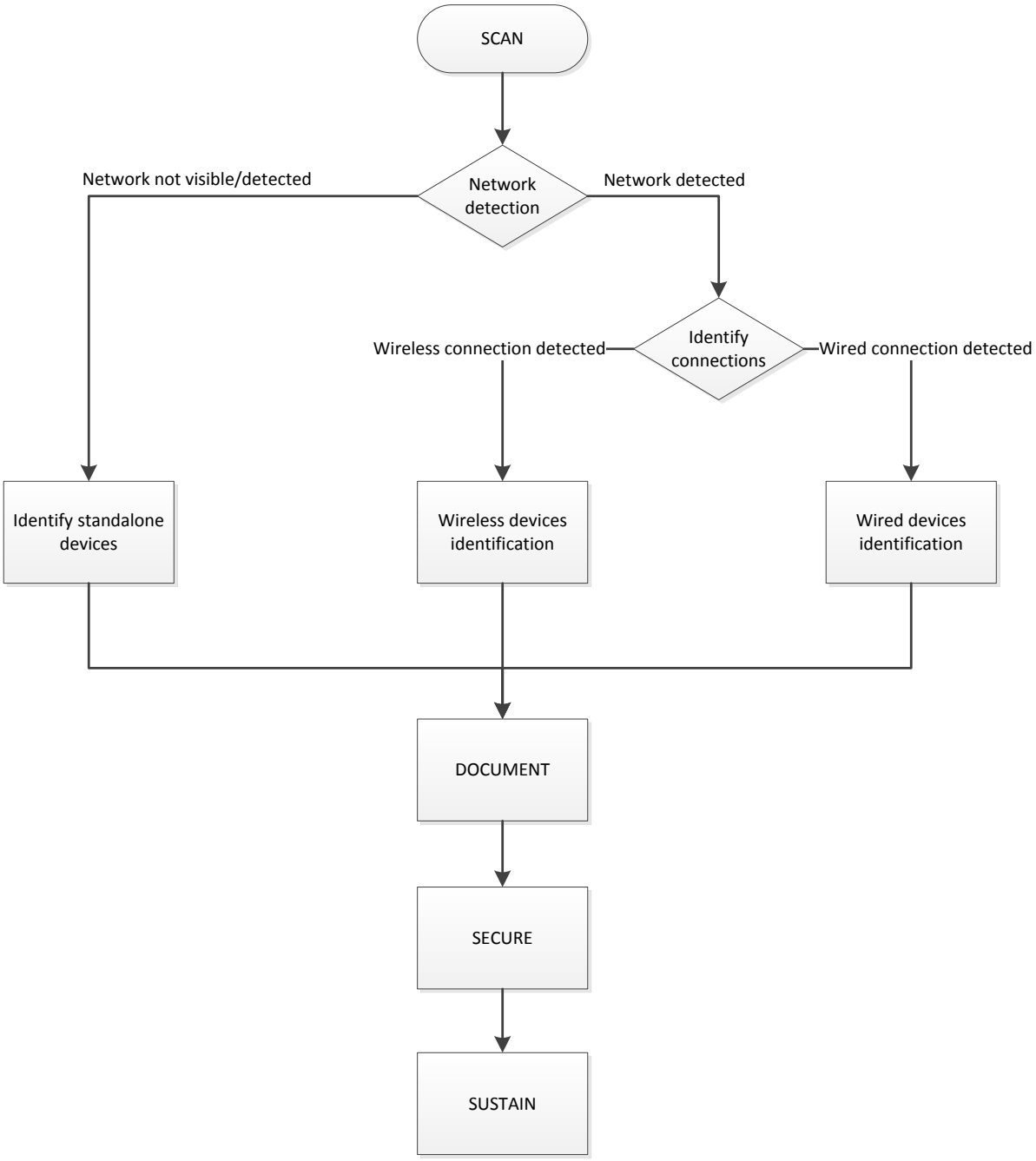
2. **IDENTIFY**
    a. Identify electronic devices, all digital devices, media and connectors.
    b. Identify devices connected to any network (local or external).
    c. Examine the devices for any visible damage.
    d. Identify booby-traps, kill-switches and devices using other anti-forensics techniques.

3. **DOCUMENT**
    a. Log any visible physical damage.
    b. Video/photographically document room(s) in which the equipment is found, the front and back of the computer or sketch any physical evidence (including cords and connections) to be seized, before removing.
    c. Operators should generally avoid active interaction with the computer, unless planned (e.g., on-loading surveillance software may actually be the mission).
    d. Use labels (to include the collector's initials, date, and time), putting evidence tape on the back of the machine.
    e. List the contents of each container that is being transported, when time permits, and seal with evidence tape.
    f. Record all activities conducted and maintain a chain of custody.

4. **SECURE**
    a. Secure any printed material or hard-copy evidence.
    b. Determine if device is on or off; if on, the screen might have content of interest (take pictures). Otherwise, look for lights or sounds.
    c. Try to access volatile data content. Be aware that anti-forensics memory techniques might have been used to modify volatile content.
    d. Power down any devices only if forced to (i.e. physical extraction of HDDs) and log the time of the shutdown.
    e. Safely secure seized electronic devices and media for transport in a hard-shell case (if available), Faraday bag, packing foam, antistatic plastic wrap, or cotton cloth.

5. **SUSTAIN**
    a. Install surveillance software if conditions allow.

b. Utilise the existing internet connection or create a temporary communication channel for data extraction from the relevant digital devices.
c. Utilise wireless networks and other possible communication technologies according to the requirements of the Theatre.



Flowchart 1. Collecting digital evidence.

A visual representation of the triage is shown in Flowchart 1. Certain activities might or might not be initiated simultaneously with others: for example, pending time availability and force protection, the ***document*** phase might happen off-site, once team security is granted. Nevertheless, behind any *principle of necessity* a certain

set of measures (establishing the basis of the chain of custody, such as video-recording of the seizure) must be undertaken as a minimum to avoid damaging the admissibility of evidence. Approaches might also differ if volatile data represent the actual target. Again, first responders' judgment will establish prioritisation.

Operators should ***scan*** the environment for the variety of computers and electronic devices capable of storing information. Computers are not limited to desktops, laptops or notebooks, but also include rack-servers and raid solutions, wireless NAS, media players, etc. Hand-held devices can include smartphones, tablets, PDAs, etc. GPS, games consoles, smart televisions and printers also process and store valuable information.

Figure 2. Transparent USB drive[1].

Operators should also look for digital storage media in the form of internal/external hard drives, thumb drives, electronic cards and DVDs. Storage devices might be deliberately deceptive in appearance, implementing anti-forensics measures[2] and assuming the form of a Swiss knife, cork bottle stopper, transparent USB memory drive (see Figure 2), etc. Miniaturisation enables a significant amount of information to be stored in solutions that are almost impossible to retrieve in compressed site exploitation operations.

During the scanning, a computer network can be detected from modular RJ45 connectors plugged into network interface cards (NIC) or a positive result from wireless signal detection devices. Discovering a wireless network, in particular, can have a major payoff, due to the physical proximity of the connected computers and hardware: large capacity wireless hard drives might be hidden from view but contain valuable records for intelligence exploitation purposes. With the current forensics tools, the SOF might not be able to detect everything during the operation. For example, scanning the number of networks to create an estimate of devices present may give a clue to hidden devices, but it is much easier to create fake networks than to detect them. Booby-traps and kill-switches may be present, also including hidden and obfuscated devices. In the worst case, some electronic devices might contain bombs that are not discovered during their seizure. As the technical exploitation begins, particular caution should be applied in case of possible usage of anti-forensics techniques, including explosives. It is therefore important to document discovered techniques and suspicious evidence before turning over materiel for analysis.

[1] Figure from *http://www.bitrebels.com/technology/polytron-transparent-usb-flash-drives/*
[2] Various types of devices are listed also in paragraph 7.1- 'Data and Device Hiding'.

Figure 3. A faulty laptop explosive device used in a 2013 attack on Mogadishu, Somalia[3]

Once the scan is complete and the networked environment assessed, the ***identification*** of computers and electronic components follows. Interactions with running electronic devices should be limited, focusing on their status, assessing eventual damage, beginning the process of seizure that needs to be documented by video-recording or photographs (if security conditions permit). It is extremely important to identify and collect electronic devices, cords, cables and connectors in order not to run into power supply issues when technical exploitation is initiated. All manuals or other printed materials related to the electronic devices should also be considered during the identification.

Successfully preserving digital intelligence for forensics analysis goes along with the establishment of a proper chain of custody. This represents the basis of the ***document*** phase of the triage. Video/photographs should be taken of the front, back and sides of all computers and devices that are discovered, before they are touched or moved. A voice-activated audio recorder (if not a wearable video-camera) would be the best alternative to any logging/sketching activities when time and safety are critical. While conducting highly compressed combat operations, establishing the chain of custody might be initiated once the safety of team members has been assured. In the likely scenario of devices to be exfiltrated out of the site, they need to be ***secured*** for transportation. This is actually one of the most sensitive activities performed on site, given the fragility and volatility of data, and requires a triaged approach based on different scenarios (covered in Chapter 8 - 'Exfiltration Solutions'). Identified devices might vary in portability and status (powered-on/powered-off) determining different actions for securing data. Powered-on devices offer opportunities for volatile data (running on RAM) dump: nevertheless, the minimum interaction with devices should be observed in order not to alter digital evidence. Devices to secure should be packaged in antistatic material, preferably Faraday bags, to prevent any remote access command or related anti-forensics measures (such as wiping). Any electronic devices must be kept away from magnets, moisture and radio signals. Enabling power supply to keep memory processes running should also be considered during the strike preparation.

[3] Figure from *http://edition.cnn.com/2016/02/11/africa/somalia-plane-bomb/*

Figure 4. Faraday Cage[4].

The ***sustain*** phase represents the new frontier for intelligence-gathering purposes. In planning the mission, an accurate cyber-intelligence preparation of the battlefield (C-IPB) could reveal the presence of enemy critical information that will be difficult to extract because of device portability or accessibility; as an example, this is typical of data centres. Installing surveillance software on targeted devices and operating data exfiltration through swiftly established wireless networks may represent a valuable alternative. The challenge is composed of a combination of factors, ranging from the possibility of targeting (with malicious payloads) complex server solutions to the survivability of the deployed networks that could operate even beyond the strike duration. Chapter 9 – 'Sustaining the Data' covers the matter in more detail.

[4] Figure Courtesy PARABEN.

5 Onto the Battlefield

Christian Braccini

The asymmetric threat environment where SOF operate includes *expected* or *unexpected* exposure to electronic devices and storage media being used by the enemy to process critical information. The opportunity to target the enemy's Battlefield Internet of Things, either for intelligence exploitation or legal actions against illegal combatants/criminals, lies in the digital forensics capabilities of combat-compressed operations, typical of SOF. These capabilities begin with SOF operators *scanning* and *identifying* the digital assets for transport, then eventually turning them over to forensic specialists and intelligence analysts for technical exploitation [1]. Having established a proper chain of custody would be the key for any criminal prosecution.

SOF will have to deal with a complex set of procedures where different variables influence the overall success of digital media collection. The triaged approach, as proposed in this monograph, aims at maximising the effectiveness of decisions to be taken in combat-compressed operations that are likely to be also technical exploitation operations. Far from turning SOF operators into IT experts, the maximum use of automation and the latest technological findings, in terms of deployable architecture supporting data extraction, show the way for SOF to achieve accuracy, agility and rapidity when it comes to digital data collection.

From this narrowed approach, focused on SOF operating in the battlefield, different scenarios might be derived ranging from homeland counterterrorism to more conventional investigations. Different constraints, in terms of survivability on the ground and technological support available, might therefore require specific tailoring of digital forensics procedures as proposed in this study.

The chapters that follow are intended to describe in more detail the role of technology in leading digital intelligence and evidence collection on the battlefield. Opportunities lie on both sides, the ally and the enemy, where the effectiveness of digital forensics techniques and the sophistication of supporting architectures confront the equivalent, advanced anti-forensics response of the opponents. The insights presented here aim to support the different principles constituting the SIDSS triaging model: the IT architecture estimation of the target infrastructure including anti-forensics measures potentially in place (*scan*); the most effective procedures for physically extracting hard disk drives; expeditionary wireless ad-hoc networks supporting a surveillance software-driven exfiltration of data (*secure*); and how to conduct the operation in line with the legal framework and create a chain of custody.

In particular, the following chapters contain the present information:

- Chapter 6 – 'Computer Forensics' covers in detail the technical architecture supporting SOF digital forensics tasks. It also includes a description of the information statistically gatherable during analysis, providing guidance for the SOF team's prioritisation of acquisition.

- Chapter 7 – 'Anti-Forensics Measures' covers anti-forensics measures that the SOF should be aware of. It concentrates on opposing techniques used to make the *scanning* and *identification* of evidence more difficult; it also describes techniques that can be used by the enemy after the collection, for example to wipe the evidence or to destroy forensics investigation tools.

- Chapter 8 – 'Exfiltration Solutions' describes different data exfiltration scenarios for SOF digital intelligence collection operations. Simple flowcharts with explanations clarify the SOF operator's decision on how to proceed if a specific type of device is *identified*. Basic mechanisms for how to *secure* an electronic device that represents potential evidence are included in the chapter as well.

- Chapter 9 – 'Sustaining the Data' gives an overview of requirements and possible technological alternatives for the establishment of an information channel during the *sustain* phase of the SIDSS triaging model. This

channel enables the SOF operators to automatically extract forensics data during and after the operation, by using the existing internet connection of the digital devices or network components swiftly established in the theatre.

- Chapter 10 – ‘Chain of Custody’ describes the legal framework for operations in general and specifically the preparation of the chain of custody, how to prepare proper documentation and how to handle evidence.

6 Computer Forensics

Agostino Panico

As mentioned by Lorge in [4], in the past, a unit would probably have cleared a building and moved on, or detonated an improvised explosive device, but today they might dust for fingerprints, take water bottles for DNA testing, and collect other evidence first. The same can happen for digital forensics.

Perry describes computer forensics as follows: 'Computer forensics involves the identification, extraction, documentation, preservation, and interpretation of computer data.' [1] Computer forensics actually begins when SOF operators scan and identify the digital assets for transport, and then eventually turn them over to forensic specialists and intelligence analysts for technical exploitation. Digital information seized as a result of special operations might be used for intelligence-gathering, typical of technical exploitation operations. It might also serve as evidence in legal proceedings, typical of evidence-based operations (EvBO). For the latter, a well-documented chain of custody is therefore fundamental, as detailed in Chapter 10 – 'Chain of Custody'.

This chapter first introduces computer forensics and then details the technical architecture supporting SOF digital forensics tasks. It also describes the information statistically gatherable during the analysis, providing guidance for prioritisation in any SOF team acquisition.

6.1 Computer Forensics: Introduction

Digital forensics has consistently been used by law enforcement, resulting in procedures, rules and best practice continually being developed. Nowadays, the minimum requirements for handling digital evidences are well established.

Digital forensics has also featured in fiction, in the criminal investigation context. This might have led to a misleading idea of digital forensics as a point-and-click feature, with which any kind of information can be retrieved in a matter of seconds. Unfortunately this is not completely true.

In this monograph, the more restricted scenario of battlefield digital forensics is considered rather than criminal scene digital forensics. SOF operates in the context of combat-compressed operations, where different dynamics apply in comparison to law enforcement.

This potentially makes the acquisition of evidence an issue, if police investigation best practices are to be used in the battlefield. In addition, it is noteworthy that there is no publicly available and updated source that explains how to carry out data acquisition in a hostile environment.

There are a number of general principles that underpin the *collection* and *preservation* of digital information seized during operations. The SIDSS acronym captures the essence of what should be performed by SOF.

Force protection always comes first. Next, actions taken regarding electronic information should avoid creating or causing changes or damage to electronic evidence. Personnel should have basic knowledge of how to acquire digital information. Appropriate tools should be used when possible. All steps taken to preserve the digital evidence collected should be fully documented, including pictures and/or notes when possible. Documentation of the scene should possibly include the entire location – for example, the type and the position of computers, their components and peripheral equipment, and other electronic devices. These activities can be done later after combat action, once security is assured and probably off-site.

Best practices for conducting forensics computer operations are as follows:

- train personnel in basic computer forensics and anti-forensics techniques;

- prior to the operation, gather needed tools and a supply of packaging materials that will help to assure the safe removal of the digital devices and media;
- define the technical architecture supporting a data exfiltration operation;
- prepare any preliminary paperwork;
- brief personnel on any expected *digital evidence* or information that might be recovered;
- designate at least one forensics computer specialist to be in charge of prioritisation of the acquisition;
- identify computer and electronic devices and media;
- avoid interacting with the computer or executing any programs based on instinct;
- document computer and electronic evidence by labelling, photographing, or sketching after the action;
- package all electronic devices, media and other transportable evidence to be exfiltrated;
- remove and transport evidence and protect the physical integrity of the components.

6.2 (SOF)DFA and (IT)Target Infrastructure (ITTI)

The previous paragraph has introduced the basic requirements needed for the acquisition of digital forensics evidence in a hostile environment; this operation should be supported by an infrastructure designed with this scope in mind. This paragraph will describe an overall architecture that can be used to address this problem. At the moment there is no technical solution specific for this, so this document provides a possible implementation, highlighting the limitations that can be faced. First of all, the technical infrastructure supporting the SIDSS process should be defined.

(SOF)DFA: (Special Operation Forces) digital forensics asset. This term includes the set of DF trained operators, the technology used and the procedures adopted to achieve the specific task of digital information collection during the strike. The analogy that comes to mind is the medical asset present in any military operation: in the same way, the forensic asset should allow operators to perform a correct triaging process based on the SIDSS model explained in the previous pages.

ITTI: Information technology target infrastructure. This term describes the IT Infrastructure present in the environment to be targeted, which is heterogeneous and unpredictable in nature. The first statements of these environments will be covered in the following part of this chapter, by using real case scenarios, as detailed in Chapter 8 – 'Exfiltration Solutions'.

6.2.1 (SOF)DFA

The technical architecture supporting the SOF team can be implemented in many different ways, using different types of technology. This paragraph analyses some possible implementations, classifying them based on the connectivity linking the operators.

6.2.1.1 Ad-hoc Mobile File System

The first method is based on a project in development at La Sapienza, University of Rome, which is a work in progress but is relevant to the object of this infrastructure.

The proposed infrastructure is based on an ad-hoc mobile file system, which can be used to support the data exfiltration operation and also to guarantee the intra-team data backup that is one of the basic requirements of the DFA module of the SOF Team. More information about related file distribution research can be found from [5][6][7][20].

Unlike the conventional infrastructure-based wireless network, an ad-hoc network, as a distributed wireless network, is a set of mobile wireless terminals communicating with each other without any pre-existing fixed infrastructure. The mobile wireless ad-hoc network has several unique features that challenge the network operation, such as the routing algorithm, attack vectors, quality of service (QoS), resource utilisation, etc.

In a wireless ad-hoc network, all the nodes are interconnected by single-hop or multi-hop wireless connections. There is no centralised control or base station to coordinate the behaviour of each node in the network. As a result, each node must be self-configurable in order to adapt to various network topologies. Nodes can assist in transmitting packets from a source to a destination through wireless connections in a fully peer-to-peer fashion. At the same time, because of the wireless connections, service coverage and bandwidth availability become critical issues in the wireless channels.

A main feature of ad-hoc networks is that all the nodes in the network have the freedom to move around, which causes the network topology to change dynamically and unpredictably.

Mobile ad-hoc networks that include specific gateway nodes towards other networks (such as cellular, satellite, or WiMAX) can be called hybrid mobile ad-hoc networks [8]. Some ad-hoc network routing protocols provide delay-tolerant (or disruption-tolerant) networking (DTN), and this could be used to create an ad-hoc mobile file system. DTN works over existing protocol stacks in various network architectures and provides a store-and-forward functionality [9]. One use case for DTN is military battlegrounds where the disconnection may be caused by mobility of vehicles, forces and devices, environmental factors, intentional electronic jamming done by the enemy, or by the loss of the acquisition vector. DTN can be considered as one technique used in opportunistic networks. Opportunistic networking is more flexible than DTN, because opportunistic networks may also contain other communication techniques than protocols used in the internet, and each single node acts as a gateway[5] [10].

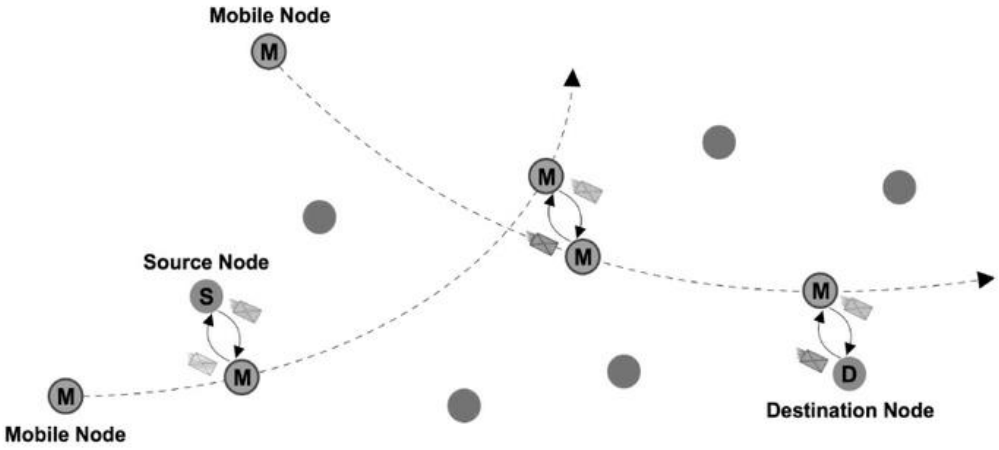


*Figure 5. DTN example of store-and-forward functionality [*11*].*

Use cases presented in Figure 6 combine a few example techniques adopted in hybrid mobile ad hoc networks, DTN-based networks, and in opportunistic networking. The idea of the figure is based on figures of [11], but includes more detail. In the figure, source S1 sends a message to destination D1, source S2 sends a message to D2, and source S3 sends a message to D3. M2 is connected into a wireless ad-hoc network which is moving with it. Originally the ad-hoc network is larger, containing a number of static wireless sensors; when the M2 moves far enough away from them, the wireless ad-hoc network is distributed into two sections. DTN allows transferring data nodes that do not have routes between each other, for example if they are located in two separate ad-hoc networks.

[5] Note that 'gateway' here does not mean the same as gateway in hybrid mobile ad-hoc networks.

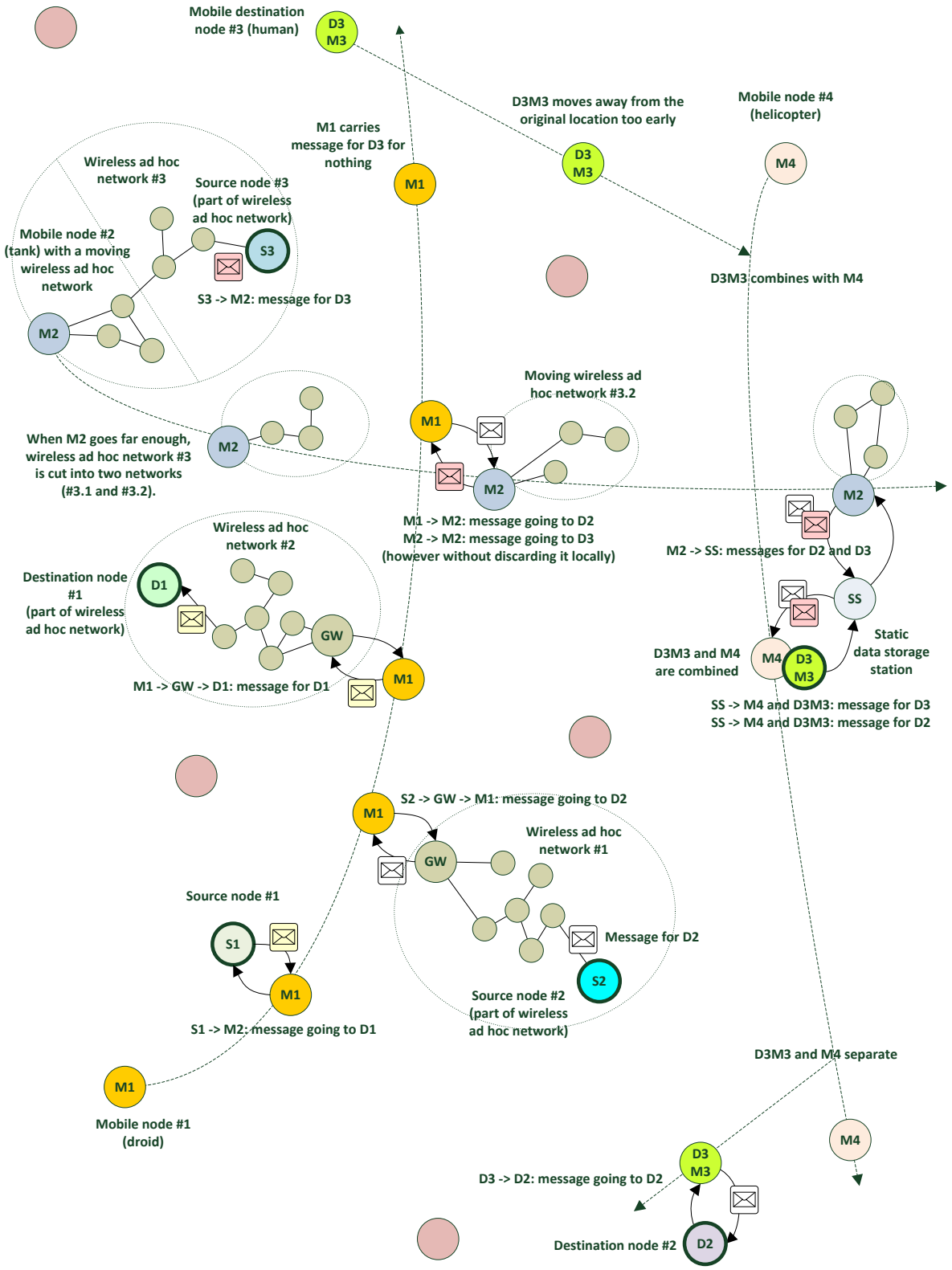


Figure 6. High level examples of DTN-based and opportunistic networking.

In a partitionable mobile file storage system, all the mobile nodes need to be managed so that all the file blocks are stored reliably against the network partitions.

Ideally, when one node is requesting to store a file in a storage system, the obvious solution is to keep the file blocks as physically close as possible, so the network bandwidth can be minimised for this storing process.

However, this solution is impossible due to a couple of issues. First, all the nodes in the storage system can request these file blocks, from anywhere at any time: even though the storing process is optimised locally, the retrieval process will be hectic in the system. Second, all the nodes are constantly moving in wireless ad-hoc network. The temporary physical neighbours may be farther apart from each other a while later; then it is rather complicated to keep track of all the file blocks in this mobile network and the retrieval process is not straightforward, either.

In the SOF operating environment this kind of network implementation might be really useful, but needs additional mobility. By making extensive use of drone technology, an adaptive strategy is proposed based on a moving swarm of drones, with a high degree of security and reliability even if drones get captured or compromised. Such a distributed solution can act as a base software platform allowing the implementation of domain-specific applications.

Security, reliability, performance and scalability are the keywords that properly define a secure distributed information system. Mobility, flexibility and re-configurability make drones the best choice for SOF mission assurance.

This configuration considers a secure distributed information system based on a swarm of disposable drones. The system grants adaptive security without requiring physical protection of the drones themselves. Although an attacker can intercept data communication between drones (passive attack), can capture a drone collecting its contents, or can compromise and substitute one or more drones with malicious ones (active attack), the attacker cannot really intercept information due to the distributed file system.

The proposed system is adaptive in two dimensions:

- a physical dimension, where drones automatically reconfigure their network topology based on client request patterns, drone failures and drone compromise.
- a virtual dimension, where data files are shared and moved between the drone nodes to guarantee an adaptive and secure file allocation.

The Dipartimento di Informatica of La Sapienza University has called the proposed system DAISY (Drone Adaptive Information System). The swarm will be devised in such a way that it will reconfigure based on request patterns and drone failures in order to provide a reliable information system. The swarm would act as a mobile ad-hoc network, providing a high level of flexibility and re-configurability with links created opportunistically to maximise the performance, as well as the resilience, of the network. In this scenario, the drone nodes will provide their clients with both connectivity, through a secure ad-hoc network, and access to stored information that is distributed between the drones themselves. Each drone therefore acts as both a network node and a mobile storage facility.

A crucial point in this setting has to do with the energy required for the communication between drones as well as their individual movement. The problem of energy-efficient routing has already been addressed in the literature [12], however this solution does not take into consideration the energy cost of drone movement. In particular, the drone movement itself could be exploited to dynamically replace discharging drone nodes with charged backups in an incremental fashion. According to the properties of the presented adaptive file allocation protocol, the content of the backup drone should automatically converge and synchronise with the rest of the swarm.

Another issue lies in the coordination required to cope with the interactions between the drone flying control and the adaptive data allocation. Controlling the entire swarm movement as well as each drone’s dynamic placement in the network is an extremely hard task for human control. To address this, the study intends to rely on state-of-the-art machine learning techniques to train swarms of drones to adapt and respond to various changes in the domain.

This system communicates with operators on the ground equipped with proper exfiltration vectors. The evaluation of the possible compatible vectors will be explained in the following paragraph.

6.2.1.2 Stand-alone Exfiltration Point

Another potential infrastructure implementation is the stand-alone exfiltration point.

This option is obviously the cheapest and easier to implement from a technological point of view, but from a tactical perspective it represents a big issue: the acquired information is stored in a single point, aka the exfiltration vector, which is also the single point of failure of the acquisition chain. All the vectors that are compatible with this option will be described in the following paragraphs.

6.2.1.3 Vector Options

As mentioned above, one of the critical parts of the entire infrastructure is the vector used by the operator, which should have some particular characteristics, such as portability, cross-platform architecture, plug-and-play solution (as simple as possible). This part of the study presents ways for the vector to be implemented, which need to fit in the overall DFA:

- USB: the simplest way to choose is, without any doubt, a simple USB drive. This solution is the easiest to implement but is also the one that represent the biggest point of failure, because it fits with the stand-alone exfiltration point given to the operator; however, the USB should be able to connect with a number of heterogeneous devices, and should execute code capable of a forensic acquisition of volatile data on a lot of platforms, with minimum interaction from the SOF operator.
- USB+: this solution is based on the USB but goes a step further; it represents the minimum requirement to support the ad-hoc mobile file system and guarantee intra-team backup, in such a way as to avoid the single point of failure of the simple USB drive. This solution should be able to communicate with the exfiltration infrastructure with a main channel, which can be a Wi-Fi connection, and a backup channel such as Infrared or Bluetooth. As well as having all the characteristics of the USB described above, the USB+ should also implement some anti-forensics techniques (as described in Chapter 7 – 'Anti-Forensics Measures'), to limit the amount of information that the enemy can eventually gather from (SOF)DFA infrastructure. This requirement is mandatory because, as will be shown in paragraph 6.3 on statistical gatherable information, the implementation of anti-forensics techniques drastically reduces the information that can be acquired. Another aspect that should be covered is the opportunity of the *sustain* part of the triage as will be explained in Chapter 9 – 'Sustaining the Data': this solution is intended to deploy the malware used to create persistence in the network.
- Wearable Options - Battlefield Internet of Things: The last option described is a cutting-edge version of the common wearable technology: this option should be able to meet all the requirements including physical ones. This option can fit the Smart Dust Sensor solution, covered in Chapter 9 – 'Sustaining the Data'.

6.2.1.4 (Architectural) Minimum Technical Prerequisites

The previous part of the chapter described some options to build the architecture to support the DFA in SOF operation. This paragraph summarises the minimum technical requirements, whatever technology is being used:

- Intra-team backup: The information acquired is invaluable and can help future missions and save many lives; for this reason it is essential to have the capability to store information not in a single point, but in the infrastructure itself. Using a DTN-based Mobile Ad-hoc Network (MANET) can be the best option.
- Easy to Use: The timeframe of the SOF raid is limited, meaning there is no time for troubleshooting. Architecture should be stable and the exfiltration vector should privilege maximum automatism.

- Connection Backup: The vector should be able to use multiple types of connections, from wired to wireless, to assure the acquisition of the information in major cases.
- Leave no trace: This technology is an asset for the operators, but can become an asset for the enemy, meaning that anti-reversing techniques should be used to reduce the risk of losing this advantage.
- Portable: The vector should be portable and should be able to operate without power as long as the mission lasts, using cutting-edge power-saving technology.

6.2.2 (IT) Target Infrastructure (ITTI)

The target infrastructure is the enemy IT environment that the operators are going to access during the mission. The entire supporting architecture (SOF-DFA) should be optimised if specifications of the ITTI are known before the mission. All the possible scenarios will be covered in Chapter 8 – 'Exfiltration Solutions'.

6.3 Assessing Gatherable Intelligence

This paragraph covers one of the most critical issues for SOF-DFA: prioritisation. This issue, mostly deriving from the limited timeframe of the SOF operation, can be addressed by using a statistical approach.

Nowadays one of the critical assets of our society is represented by 'information', which is basically nothing more than sequences of '0' and '1' stored on any kind of support, so as to be reused later. Such electronic data can be permanently or temporarily stored on chips in computer memory or on secondary storage devices. Random access memory (RAM) (usually located inside the device) stores information that is volatile; RAM retains data only as long as it is receiving power.[6] RAM is usually connected to the internal motherboard of the computer; this means that the RAM, if detached, becomes useless, although useful information about the nature of the enemy's devices and systems could be gleaned from it. The second type of internal memory is known as read-only memory (ROM); the main difference from RAM is that it is non-volatile, because it is embedded: ROM chips are usually found inside the computer and the instructions contained on a ROM chip are executed when the device is powered on. Nowadays it is commonly called firmware and can be used to preserve information if attacked, as covered in Chapter 9 – 'Sustaining the Data'. The information acquired from the computer or created by users represents an invaluable asset for anyone who has to make a possible information acquirable analysis. However, some data is volatile while being processed, transmitted, or stored; turn off the power at this point, and the data disappears. A basic summary of electronic information characteristics follows; this will be critical for understanding how to give priority to device acquisition:

- *Storage media* includes external hard drives, CDs, DVDs, SD disks or flash memory, USB drives, network storage devices, and wireless storage devices;
- Information that is stored in RAM or ROM is referred to as *primary storag*e or *memory*.
- Preserving the integrity of digital data involves the careful collection and documentation of digital media storages. For example, data that is recorded on storage and exposed to magnetic or electromagnetic fields can be altered or destroyed and lost forever.

An important set of characteristics that should be taken into account in a BDF scenario are the limits that are imposed by the environment or the mission risk; for this reason it is really important to prioritise the devices to seize in order to have the best chance of successfully gathering the available intelligence. Deception and anti-forensics techniques make it even harder.

[6] Cold boot attacks can be used to increase the time, read more from https://www.technologyreview.com/s/530186/the-ongoing-threat-of-cold-boot-attacks/.

In order to achieve this goal, the following part of this chapter covers the statistical analysis of the information present on different kind of devices. It should be underlined that the approach is based on empirical data mixed with a statistical overview, and the results can change if correlated with information-gathering about the ITTI.

When collecting evidence, it is recommended to proceed from the volatile to the less volatile. This is an example of order of volatility for a typical system:

- registers, cache;
- routing table, address resolution protocol (ARP) cache, process table, kernel statistics, memory;
- temporary file systems;
- disk;
- remote logging and monitoring data that is relevant to the system in question;
- physical configuration, network topology;
- archival media.

The goal in this study is to assure, statistically, that the gathered information is the most comprehensive possible, in a way that can lead further operations.

To reach this goal, an algorithm to assist in determining the major possibility of information gathering is needed.

For this algorithm the following information is needed in order to carry out the statistical analysis:

- Effectiveness: in percentage terms, the likelihood of the device containing useful information;
- Level of effort / resources: estimated time to perform prioritisation based on small, medium and large estimates;
- Compatibility of toolsets: the amount of time in minutes to adjust or install the prerequisites for this device;
- Familiarity with devices and this toolset: based on descriptions of novice, experienced, and expert.

The first step to take in addressing the statistical analysis is to obtain the needed parameters, defined as follows:

- Effectiveness: this parameter should cover how effective an acquisition of a different type of device can be;
- Acquisition time for dataset size: this parameter should address the amount of data that can be acquired in the mission amount of time;
- Additional costs are ‘converted’ to minutes to adjust methods that require an additional set-up time or resources: this parameter should cover the troubleshooting time needed in case of tools failure;
- Power status: this parameter should cover the power status of the device, in case of a portable device this parameter is critical, but the risk can be reduced using an external power supply;
- Connectivity: this parameter should cover the connectivity status of the device, this evaluation should be done before the acquisition, also because, as explained in Chapter 8 – ‘Exfiltration Solutions, the acquired device should be stored in a ‘safe place’ to avoid enemy interaction with it;
- Anti-forensics measures: this parameter should take into account the statistical degradation of information if an anti-forensics measure is in place, to understand and recognise anti-forensics measures (see Chapter 7 – ’Anti-Forensics Measures’).

The study starts by addressing which kind of device is most likely collectable from the operators on the ground, as the first step of the analysis. From this algorithm, the statistical gatherable intelligence is calculated.

The goal of this statistical approach is to measure effectiveness of information gathering from a device, based on what can be identified in the environment using the SIDSS process.

The first definition of this approach can be outlined as follows:

'f(x) = (log2(1/(1-effectiveness)) – (AcquisitionTime + personTime + 0.75 * additional_Effort))*(Power)*(Connectivity)*(Antiforensics_Measures)'

Obviously this algorithm cannot address all the parameters and in particular the operating environment of SOF operators, but it is the first to try to address the problem.

Based on this algorithm, a list of gatherable information is presented, which will be useful to address the prioritisation problem that the operator faces while in action. Any further consideration can be made and extended based on the same logic and operator's experience.

Table 1 shows the statistical intelligence that can be gathered according to the algorithm. The percentage represents the possibility to obtain relevant information from the device. All the percentages take into consideration the usual dimension of devices impacting the mobility and the opportunity to carry the device; the effectiveness has been calculated based on the state-of-the-art acquisition methods used by law enforcement. The additional cost is added based on a Gaussian distribution as well as the acquisition time, about 5 minutes.

Table 1. Statistical Gatherable Intelligence Table, based on Chapter 8.

Statistical Gatherable Intelligence					
	O.S.	**Power**		**Connectivity**	**Anti-Forensic**
		ON	**OFF**	**ON**	**ON**
Laptop - Overall		67.7%	59.2%	74.9%	33.6%
	Windows	72,0%	63.1%	75.3%	35.1%
	Linux/Unix	68,0%	59.2%	70.2%	32.9%
	MacOSX	63,0%	55.4%	79.1%	32.9%
Phone - Overall		83.2%	77.6%	93.8%	42.4%
	Android	93.2%	83.2%	96.3%	45.5%
	iOS	81.2%	78.1%	93.2%	42.1%
	Windows	75.1%	71.6%	91.8%	39.8%
Tablet - Overall		83.0%	76.8%	91.5%	41.9%
	Android	91.4%	79.1%	93.1%	43.9%
	iOS	80.3%	82.3%	92.3%	42.5%
	Windows	77.4%	69.1%	89.1%	39.3%
Desktop		67.7%	57.2%	83.7%	34.8%
	Windows	72.0%	63.1%	82.7%	36.3%
	Linux/Unix	68.0%	59.2%	79.1%	34.4%
	MacOSX	63.0%	49.4%	89.3%	33.6%
GPS		55.8%	52.8%	72.5%	23.3%
Server	**Difficult to evaluate. The information is valuable, however these devices are more effective if used as foothold for the sustaining phase (Chapter 9)**				
Storage					
Wearables		91.2%	85.6%	95.3%	52.7%
IoT		82.8%	81.7%	95.3%	51.8%

6.4 Summarising the Technical Requirements

This paragraph focuses on final requirements that the DFA Infrastructure and the SOF Operator should consider to optimise the intelligence collection:

- Intra-team backup capabilities, based on ad-hoc mobile connections;
- Understanding of the basic concept of intelligence gatherable from devices based on the statistical analysis and experience;
- Understanding of the basic functionalities of the vector used;
- Understanding of the SIDSS process and the entire digital forensics process;
- Understanding the importance of documentation after action, to support the Digital Forensics Analyst.
- Knowledge of the basic anti-forensics measures that can be in place, and how to recognise them.

7 Anti-Forensics Measures

Teemu Väisänen

The use of anti-forensics (or counter-forensics) techniques is a common practice for advanced and persistent actors, particularly in the contexts of targeted attacks or efforts by organised criminals to erase digital traces [13]. It is also a technique that can be used to provide additional privacy and protection for own systems. As mentioned in 6.1, it is recommended to train personnel in basic computer forensics and anti-forensics techniques.

Anti-forensics techniques can be categorised at high-level as (data) hiding, artefact wiping, obfuscation, exfiltration, attacks against computer forensics, and booby-traps. They can also be categorised based on the achieved effect. Steganography, for example, can hide and obfuscate data, and can be used for exfiltration. Botas et al. have used taxonomy in anti-forensics techniques to consider any component of a computer that handles data: memory, computer forensic tools, network, and data [14].

Anti-forensics might include tampering with log files, using wiping or 'cleaning' tools, deploying rootkits, using hidden data storage areas, or even deploying traps to be activated in the course of a later investigation. Some of the anti-forensics techniques can be categorised as destructive processes. It should be noted that it is highly possible that, during a strike, SOF will not be able to do any analysis to discover anti-forensics techniques in place. Still, it is good to know what kinds of techniques exist at basic level and especially techniques that might affect the work done during the strike.

Captured devices might be booby-trapped[7] or configured with anti-forensics software, and this is one of the primary reasons why combat forces require training in digital forensics [15]. If possible, captured computers should not be shut down. This is because hard drives or SSD disks may be fully encrypted, or the whole OS run from a live distribution,[8] which often makes later investigation impossible. Instead, live imaging of storage media and RAM should be considered and pursued. More information about volatile memory capture is given in Chapter 8 – 'Exfiltration Solutions'. It is good to know that memory anti-forensics techniques may be present, so the volatile memory can be modified or some evidence hidden. With current forensics tools and manual analysis, there is no time to detect usage of memory anti-forensics techniques during a special operation: custom acquisition tools are required that are able to automatically check for memory anti-forensics.

Even though anti-forensics techniques provide many additional challenges for the operation and subsequent analysis, it is claimed in [15] that there have been no published reports confirming the use of effective anti-forensics techniques on the digital devices seized from terrorists. It is therefore important to seek for indicators proving external forms of support in increasingly sophisticated techniques.

7.1 Data and Device Hiding

This chapter describes data and device hiding techniques, which are useful for selected members of SOF, specifically the (SOF)DFA, to know about.

Data hiding includes various techniques such as encryption, steganography, and use of packers. It is basically impossible to detect data hiding during a strike, and this should be taken into account when designing and

[7] Booby-traps are aimed at creating uncertainty, lowering the morale of the military forces and hindering their movements, and might contain explosives [3, p. 21]. However, in this study we use the term also to include digital booby-traps intended to destroy data.

[8] As described in [13, p.36], no evidence can subsequently found on the hard drive if any Linux live distribution (live-CD) has been used.

configuring automated tools for gathering evidence, for example from computers. Data can be hidden in various locations (such as memory, slack space, hidden directories, bad blocks, alternate data streams, or hidden partitions) in a computer system. Because of this, it should be remembered that automatic tools only capture common user document folders, and some hidden but useful data is possibly left behind.

During special operations there is no time for analysing possible anti-forensics data hiding techniques; however there might be time to consider physical hiding. Storage media and small computers can be physically hidden anywhere. This might be more useful information for the SOF than data hiding techniques. For example, USB flash drives can be in the form of food, toys,[9] jewellery, or tools. A transparent USB flash drive is shown in Figure 2.

One anti-forensics technique presented by Michael Perklin [16] is dummy HDD, which means a computer with an HDD that is not actually used. The actual OS can be booted from an USB flash disk. It is possible to still write to the HDD so that it looks as if it has been used; however, during a special operation there is no time for such analysis with the available forensics tools. Perklin gives guidelines for mitigating dummy HDDs: two usable techniques are checking USB flash drives in USB slots (and pending time availability, also on motherboards, see Figure 7) and monitoring network traffic before seizure to detect remote drive locations.[10]

Figure 7. Example USB slot in a motherboard[11].

A 'redundant array of independent disks' (RAID) is used in storage systems to prevent data loss in case of hardware defects on a hard disk and to improve I/O performance [17]. When using RAID 0, only the latter can be achieved. If the enemy is using only data stripping with RAID 0, all the disks used in the setup need to be collected. With other RAID types providing fault tolerance, capturing all disks might not be required. Because of this, the enemy could use physically distributed and/or hidden RAID disks to make analysis in the laboratory harder or impossible. It is worth noting that RAID also causes other challenges, for example if specific drivers or controllers have been used to create custom RAIDs.[12] In such cases, it might be easier to collect the full computer; however, if this is not possible, tools can be used to detect parameters to reassemble the logical RAID volume.[13]

- Recommendation: Be aware that computing devices do not necessarily look like computers (the *scan* and *identify* parts of triage).

[9] For example Lego bricks, rocks, lamps, beverage coolers, coffee warmers, and other desktop toys may contain a USB plug and have the capacity to store information.

[10] The third one is checking if the OS was paging and if the Pagefile on USB flash drive points to network locations.

[11] Figure from http://www.howtogeek.com/201493/ask-htg-can-i-plug-a-usb-device-right-into-my-motherboard/

[12] In [16], Michael Perklin described using custom RAID parameters as an effective anti-forensics technique.

[13] An approach to automatically detect all parameters based on block level entropy measurement and generic heuristic is presented in [17].

- Recommendation: When designing and configuring tools, be aware of the possibility of various data hiding techniques.
- Recommendation: If possible, try to do live imaging of storage media and RAM instead of only seizing them (*secure*). Note that this might take too much time to be accomplished during the special operation; however it could be possible to use additional devices and techniques as presented in Chapter 9 – 'Sustaining the Data' to transfer the live images after the special operation.
- Recommendation: If data is collected wirelessly during and after the operation via specific extractors, it should be possible to physically destroy them remotely when wanted or automatically after the data collection.
- Recommendation: Be aware that hard drives or SSD disks might be encrypted, so if possible, try to capture computers 'as is', without shutting them down or removing any storage media (*secure*).

7.2 Artefact Wiping

Artefact wiping means techniques for automatically or manually eliminating particular data, files or entire file systems, usually permanently.[14] It includes data erasure (also referred to as data clearing or data wiping), and disk degaussing and destruction[15] techniques. As mentioned in [18], artefact wiping tools make analysis more difficult for forensics examiners, but they are not perfect. This chapter describes artefact wiping techniques that the (SOF)DFA should be aware of.

If the (SOF)DFA is able to login to the OS or access an unlocked screen, and assess that destructive processes are running, the device should be immediately turned off by removing power cord or its battery including connected devices. The following example terms can indicate the destruction: 'wipe', 'delete', 'format', 'remove'; however, the system's language may not be English and destructive processes can also be done stealthily. Still, it is important to check screens during the seizure, because it is possible that a destructive technique such as data wiping is started after the forensics tools are connected to the device.

7.2.1 Wiping Data Remotely and Self-Destruction

In a normal situation, artefact wiping is done by specific cleaning tools.[16] In such situations there is no need to do it fast, but during (or after) the operation, the enemy may use faster, more automated, and remotely working techniques. This chapter describes self-destruction techniques and techniques usable for remotely wiping the data.

As described by Jane Wakefield in [19], criminals have used remote wiping functions to wipe mobile devices that were seized by police officers and secured in police stations. Because of this, it is important to store devices properly immediately after capturing them. For this, anything providing the functionality of a Faraday cage is suitable.[17] However, it is good to remember that kill-switch software exists, which wipes the device if it cannot be connected or connect to a certain location in a certain amount of time. Self-destruction can be implemented in smart phones, for example, by using specific clients that connect to the management server, and if there is no connectivity, the smartphone will be wiped. Use of self-destruction functionality is not

[14] Even if the purpose is to eliminate data permanently, in some cases and with specific tools it might be possible to get information about it. See, for example, cases where formatting a disk once has not been enough.

[15] It is possible to send remote commands to disks to destroy them physically, or to use booby-traps.

[16] One cleaning tool is CCleaner, which is downloadable from https://www.piriform.com/ccleaner.

[17] Military and intelligence agencies use Faraday bags to prevent unwanted applications being invoked remotely or data altered after devices are seized. More details about Faraday bags can be found in Chapter 4 'The SIDSS Triage'.

common, as it could also wipe the data during accidents such as power loss in cell towers. Storage media[18] and other devices also exist which can be destructed physically via an SMS and have a self-destruct functionality (that is launched if the device is put into a Faraday cage).

- Recommendation: Check the number of wireless connections and devices with specific equipment to discover if storage media have integrated GSM receivers (*scan* and *identify*).
- Recommendation: Mark devices that have wireless connections (*document*). Seal the captured devices into Faraday bags or similar (*secure*).
    - Be aware that some of the devices might wipe themselves when they lose Internet/GSM connectivity (*secure*). However, because it is rare, use the Faraday bag from these two options.

Figure 8. Autothysis128t[19]

In addition to remote commands via SMSs, Autothysis128t SSD (shown in Figure 8) provides some other means of self-destruction. When the computer or the SSD is put into a Faraday cage, the SSD will self-destruct after a set number of hours of GSM starvation. It is also possible to set it up so that the self-destruct is triggered when it is removed from the SATA III interface.

Before turning any device off, it is good to be aware that the enemy might have manipulated a 'graceful shutdown' process to prevent evidence recovery. As Lance Cleghorn writes [21], many technology professionals feel compelled to shut down the computer in question through a graceful shutdown rather than remove power from the system and risk data corruption or loss of volatile data not committed to permanent storage. However, it is possible to modify the graceful shutdown process with anti-forensics techniques so that evidences can be disrupted or destroyed. This is one reason why the shutdown of the device should always be done by pulling the power plug and/or removing the battery from the device.

7.2.2 Wiping Data When Use of Forensics Tools Is Detected

This chapter presents techniques that can be used to wipe the data when the system detects the use of digital forensic investigation tools.

[18] One such approach is presented by SecureDrives. Autothysis128t SSD, presented in Figure 8, has a GSM based remote control allowing for data destruction and physical fragmentation of the NAND-Flash storage on demand.

[19] Figure from http://securedrives.co.uk.

As presented by Azadegan, Liu, Sistani and Acharya in [22], many forensics tools follow a similar pattern of activities to retrieve data from an Android smartphone. Detection of forensics tools enables various scenarios. Techniques for causing a 'sudden death', erasing sensitive data and replacing all data from the storage, are presented in the paper [22]. It is worth noting that similar techniques can be used to detect memory and other types of forensics analysis. Such detection techniques have been used by various malware. Because use of anti-forensics techniques cannot be seen outwardly from the devices, it is impossible to say if something is modified or deleted when the forensics tool is connected to the device. One approach is to use specially crafted or modified tools that behave differently from commonly used free and commercial forensics tools. Such anti-forensics techniques can also be categorised under attacks against forensics tools, if they try to harm the tool.

- Recommendation: Be aware that various anti-forensics techniques are able to wipe the storage media (*secure*).

7.3 Obfuscation

Obfuscation can be used in various places, such as in files, code, or networks. Usually, 'trail obfuscation' means creating a large amount of fake evidence around the real evidence to make the work of the investigator harder. This has to be remembered when possible evidence is recovered from the machine. One way, for example, is to create a huge amount of interesting files with random data, encrypt them with a random key, and remove them insecurely so that they can be found later by investigators. There are publicly available scripts for these, as mentioned by Phil Knüfer in [23, p. 9.], which means that even script kiddies can use such techniques.

This chapter does not go into details of all the possible obfuscation techniques, but tries to concentrate on ones that are useful to know about during a special operation.

One technique the enemy could use is data saturation. This means collecting and distributing a huge amount of media (such as CDs, DVDs, floppy and Blu-Ray disks, SD cards, USB flash drives, hard drives, SSD disks but also cell phones). In such a case, it might be impossible to distinguish the real evidence from the fake during the special operation,[20] and also to collect all the media.

Figure 9. Piles of dead hard drives[21].

[20] In a safe situation (such as in law enforcement) it would be possible to collect all the evidence, but discovering the real ones might still take too much time in the analysis phase.

[21] Figures from Flickr https://www.flickr.com/photos/jpf/152611698 and https://www.flickr.com/photos/jpf/152611490.

Another technique is to create a huge amount of wireless networks that are not actually used for anything important. Handheld devices (even smartphones) can be used to detect wireless networks using Wi-Fi and Bluetooth; however some specific wireless networks will require more sophisticated tools. The same obfuscation could be accomplished by connecting a large amount of network cables between unused devices that are just powered on (and thus their LEDs are blinking). Manually analysing such a setup to discover the real machines would take too much time.

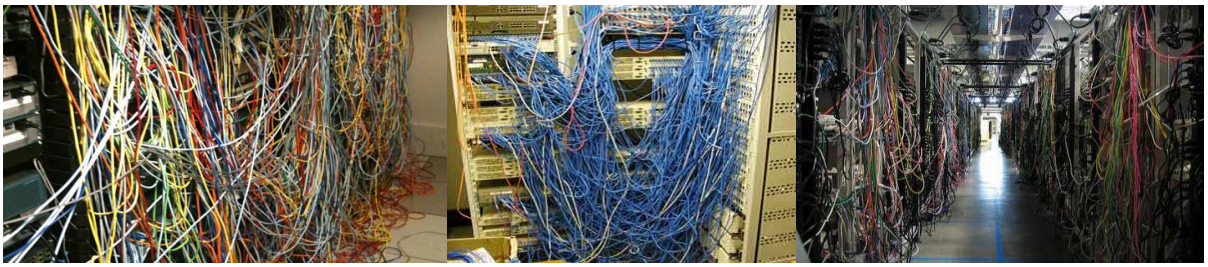


Figure 10. Examples of messy cable management setups from server rooms[22].

- Recommendation: Be aware that not all discovered wireless networks and not all blinking and wired devices are necessarily used for anything real (*scan* and *identify*).

It may not be wise to collect all switches and routers from the target site, but concentrate on more important evidence. However, it is possible to insert small computers inside empty cases, or develop specific cases for them. This could be implemented, for example, with PiZero Cluster with Raspberry Pi Zeros. PiZero Cluster and an example design of switch case for it are presented in Figure 11.

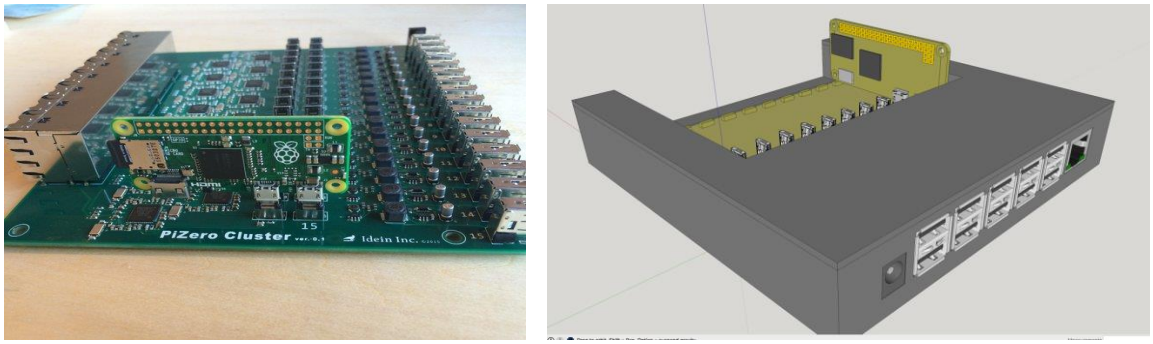


Figure 11. a) PiZero Cluster and b) an example design of the case for it[23].

Comparing a real switch rack case to a switch case that actually contains something else is challenging without opening it. There might not be enough time to open every rack case, especially if the target site includes any server rooms. Even if such anti-forensics techniques were discovered during the special operation, removing devices from server racks and carrying them might not always be possible. As also mentioned in paragraph 6.3 'Assessing Gatherable Intelligence', preservation techniques presented in Chapter 9 – 'Sustaining the Data' might be handy when servers are present.

[22] Figures from http://www.itrw.net/michigan_it_provider/server_room_spaghetti, Imgur https://i.imgur.com/fF4d9xB.jpg and from http://www.fs.com/blog/cable-spaghetti-server-room-cabling-nightmare.html.
[23] Figures from Twitter: https://twitter.com/9_ties/status/689707306494271488.

- Recommendation: Be aware that harmless-looking devices may actually include several important devices containing possible evidences (*scan* and *identify*).

In many OSs, it is possible to change the outlook of the GUI so that it seems to be some other OS. One example of a Gnome theme looking like Windows XP is presented in Figure 12. There are different procedures and specific tools that can be used only in certain OS. Because of this, tools that work in several environments could be used.

- Recommendation: Try to identify fake evidence (*scan* and *identify*). Use custom wireless scanners to detect real and fake networks.
- Recommendation: If there is no time, try not to capture obviously fake evidence (*secure*).
- Recommendation: Use specific tools to check OS type and version before using tools that work only in certain OSs.

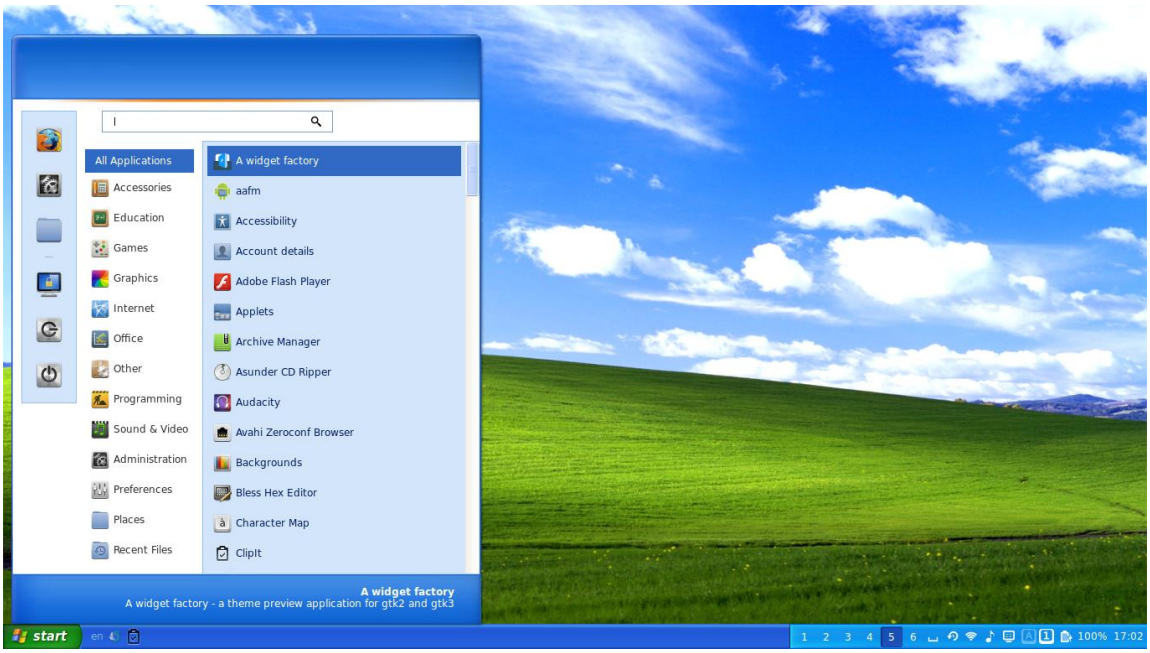


Figure 12. CinnXP-Luna theme in Linux; it looks similar to Microsoft Windows XP[24].

7.4 Exfiltration

Data exfiltration can be defined as unauthorised transfer of data from a computer. This includes techniques to evade security monitoring tools, but also techniques that can used for obfuscation, such as steganography. The same techniques can often be used for other purposes, such as for creating stealthy channels for remote controlling of devices. This chapter describes exfiltration techniques that are relevant and important to know during special operations or after them. However, after inserting the captured devices into Faraday bags, there is no need to worry about them until the actual investigation.

It is possible that some of the captured USB flash drives are actually human interface devices (HIDs). Any USB device claiming to be a Keyboard HID will usually be automatically detected and accepted by most modern OSs.

[24] Figure from http://gnome-look.org/.

One infamous example is USB Rubber Ducky[25]. Automated scripts and malware inserted into captured devices might, for example, call home.

- Recommendation: Be aware that USB flash drives might contain malware or automated unwanted scripts (*after the strike*). Because of this, content in the captured devices must be analysed in machines that have no Internet connectivity (to prevent exfiltration and calling home).

7.5 Attacks against Forensics Tools

This chapter describes detection and attacks against digital forensic investigation tools.

As described in paragraph 7.2.2, 'Wiping Data When Use of Forensics Tools Is Detected', it is possible to create software which detects the usage of forensics tools, memory analysis, etc. Scenarios presented by Azadegan et al. in [22] only contain modifying and destroying data from the smartphone; however, it is possible that the enemy may use the same ideas and hide or leave behind booby-trapped devices with electronic detonators and explosives.[26] These devices would then explode when connected into specific detected forensics tools, or taken to certain locations. Other destructive anti-forensics techniques, such as USB drives destroying (burning) hardware in computers, can also be categorised under booby-traps. More information about one example can be read in paragraph 7.6.3 – 'USB Killer'. USB flash disks acting as HIDs can be also used to attack against forensics tools. During the special operations that this study covers, it is unlikely to find hidden explosives inside electronic devices; they might be present in strikes related to counterterrorism.

- Recommendation: Before opening any device or connecting the forensics tools to it, first analyse devices to detect if they contain any explosives, for example by using colorimetric test kits, or dogs (*secure*).
    - Leave devices containing any marks of explosives behind. Follow SOF's procedures for handling explosives.
- Recommendation: After the operation and before connecting the forensics tools to the device, first analyse collected devices to detect if they contain any explosives, for example by using colorimetric test kits, dogs, or x-ray machines *(after the strike*).

7.6 Booby-Traps

A booby-trap can be a software, device, configuration of a system, or combination of these with an intent to kill, harm, or surprise a person, or to make the forensics process more difficult. This chapter describes examples of booby-traps using IT devices that SOF members should be aware of.

7.6.1 Proximity Sensors and Tags

This chapter describes how different type of proximity sensors and tags can be used as anti-forensics measures and for creating booby-traps. In addition to proximity sensors, normal wireless sensor network may be present for detecting approaching people, vehicles and other devices. More about this and using them for preserving the data from the theatre can be read in Chapter 9 – 'Sustaining the Data'.

If the authorised user goes too far from the used device, such as a smartphone or PC,[27] it is possible to protect them by locking or shutting them down or encrypting all their content. Such examples for providing additional

[25] More information about Rubber Ducky can be found from http://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe.
[26] Liscouski and McGann describe in [25] how it has been possible to insert a bomb inside a laptop.

[27] Some PC motherboards have a functionality to wake up and standby when user's smartphone (or other Bluetooth device) is close or far enough.

security for smartphones are described in [24]. These kinds of scenarios can be based on various techniques such as attaching wireless (Bluetooth, RFID, etc.) proximity tags,[28] for example to the clothes of the user. The purpose of such tags is commonly to discover things or create an alarm, for example if the smartphone or wallet is forgotten, stolen or dropped. Some tags are in the form of wearable wireless wristlet bands. It is possible to set up a system in which working on a PC is only possible if a certain tag is also present. In normal enterprise security, this would add one factor to authentication, but in special operations, the enemy might want to use the same technique to protect their information. In more advanced scenarios, heart rate monitors could be wirelessly connected to the used devices. The system could be configured so that if the heartbeat is not tracked any more, the device would, for example, shut down or encrypt the content. The same thing would happen if the device were captured (without the user) or if the user were be removed from the PC.

- Recommendation: Check the number of wireless connections and devices with specific equipment[29] (*scan* and *identify*).
    - Existing tools can be used to detect the number of networks and devices; however there seems to be no automated tools specially meant for detecting booby-traps or kill-switches. For this, specific custom tools will be needed.
- Recommendation: Mark devices with wireless connections (*document*).
- Recommendation: Check if enemy is wearing or if there are any loose small wireless tags or wristbands *(scan* and *identify*). If there are, extra caution is required. All such items, their connections and the connected devices should be documented *(document*). Captured items should be kept in proximity to the connected, captured devices *(secure*).
    - One approach is to test with one device / user pair if something strange happens when their distance is increased *(identify*). The same applies to security badges.
- Recommendation: Check if enemy wears heart rate monitors that are possibly connected to other devices to be captured (*scan* and *identify*). Mark such items (*document*). Items should be worn by the same person who captures the actual device (*secure*).
    - It is worth noting that it might not be possible to remove the heart rate monitor until after returning from the special operation.

7.6.2 USBKill

This chapter describes USBKill,[30] which is an anti-forensics kill-switch that waits for a change on a computer's USB ports and then immediately shuts down the computer. If USBKill is used, removing any USB device such as flash drive, mouse, or keyboard from the computer or inserting a new (non-whitelisted) USB device enables the computer to execute wanted commands and shut itself down. It is impossible to know during the strike what programs have been installed into computers, or what USBKill would do if currently running.

- Recommendation: If any devices that are attached to fixed solid objects (such as tables or wall) via wires going to their USB ports are discovered (*identify*), extra caution should be taken when touching (*document*) and seizing them (*secure*).
- Recommendation: If any enemy is holding, or is attached to, for example via wristbands or handcuffs, devices (mouse, USB flash drive) that are connected to computers *(scan* and *identify)*, extra caution should

[28] Various Bluetooth tags exist, such as BluTracker, Bringrr & BringTags, Chipolo, Estimote Beacon, F-Secure Buddy, Find'Em Tracking, Gecko, Guardian, PebbleBee, PROTAG Elite, StickNFind, Tile, Linquet, Locca, Lupo, TrackR, Wallet TrackR, and XY Find-It.

[29] Open source tools such as NirSoft's BluetoothView can detect Bluetooth devices. Various commercial network monitoring solutions exist.

[30] Source code and more information about USBKill can be found from https://github.com/hephaest0s/usbkill.

be observed. However, solutions for preventing the enemy from pulling out an USB flash drive from the computer might be limited.

7.6.3 USB Killer

A 'USB Killer' is a USB device for 'frying' a computer it is plugged into. As described by Adarsh Verma in [26], version 2.0 of the USB Killer dumps 220 volts directly onto the USB signal wires. Such a voltage can destroy the motherboard of the computer. By hiding these kinds of devices or leaving them behind, the enemy could destroy computers used for investigation, or at least make the forensics process slower. An example soldering of a USB Killer by hand is presented in Figure 13. If one of these is inserted into a regular USB flash drive case, obfuscation detection without opening the case is basically impossible.

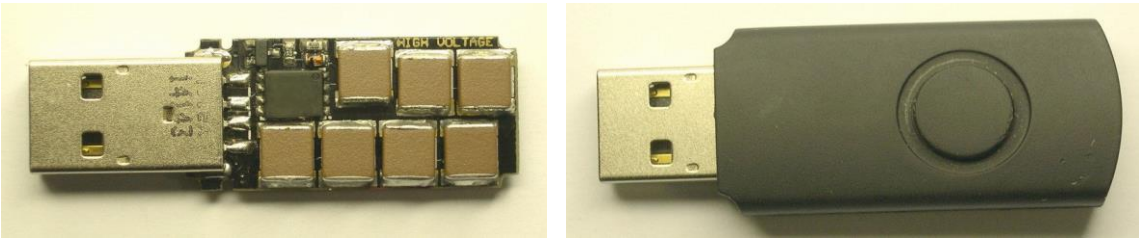


Figure 13. a) Hand-soldered example of USB Killer and b) the same device obfuscated to look like a regular USB flash drive.[31]

- Recommendation: After the collection, open USB flash drives and other USB devices to discover if they include any strange soldering, circuit boards or parts (*after the strike*).
- Recommendation: After the collection, do not connect USB devices into expensive forensic analysis devices, but first try them with testing computers which do not contain anything crucial (*after the strike*).

7.7 Summary of Anti-Forensics Techniques

In the *scan* phase, it is important to scan the number of networks to make an estimate of the devices present. This should be compared later to the number of identified devices. However, it is possible to create a large number of fake wireless networks, so normal scanning tools may not provide good enough information. This means that the SOF(DFA) should have a tool (in a handheld device) for automatically scanning and analysing the wireless traffic, and not only for discovering Wi-Fi or Bluetooth APs or devices. To decrease the number of (fake) wireless networks, it would be possible to use handheld short-range wireless jammers.

In the *identify* phase, the SOF(DFA) should discover and identify possible booby-traps, kill-switches, and hidden and obfuscated devices before starting the identification process presented in Chapter 8 – 'Exfiltration Solutions'.

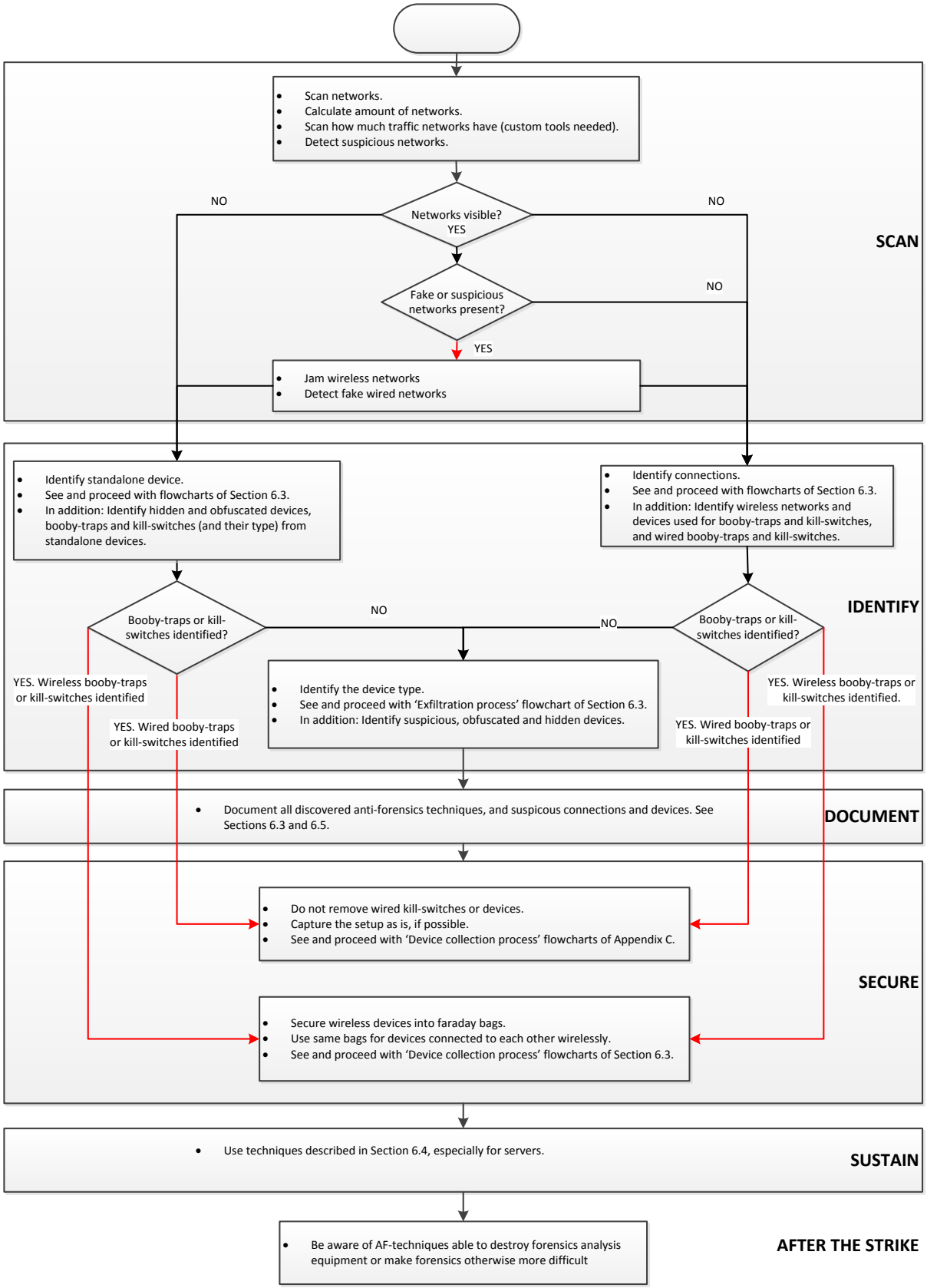
Flowchart 2 presents the SIDSS triage mitigation in case of anti-forensics measures detected: even though some arrows in the flowchart go through the *document* phase, this does not mean that related evidence would not be documented. In the *document* phase, all identified devices and anti-forensics techniques should be documented, provided there is enough time.

In the *secure* phase, the normal procedures presented in Chapter 8 – 'Exfiltration Solutions' should be followed. For example, if the device is turned on and stored in a Faraday bag, a battery must be provided. Exceptions may arise if booby-traps or kill-switches have already been discovered in the *identify* phase.

[31] Figures from http://kukuruku.co/hub/diy/usb-killer.

If any marks of explosives are detected from the electronic evidence in any phase, the evidence should be left behind. After returning from the theatre, there is more time to analyse possible use of anti-forensics techniques. For example, possible booby-traps should analysed and they should not be directly connected into the most valuable forensics analysis devices.

As mentioned already, certain activities might or might not be initiated simultaneously with others. Discovered anti-forensics measures are presented as red arrows in the flowchart. Examples are identified booby-traps, kill-switches, fake networks, and hidden or obfuscated devices. Black arrows, on the other hand, mean that anti-forensics techniques have not been discovered (in that part). For example, if there are no wireless networks visible or detected, it is still possible to identify powered-off stand-alone devices. These devices might have wireless interfaces that can be used to control devices remotely (after they have been powered on).



Flowchart 2. Anti-forensics mapped to SIDSS.

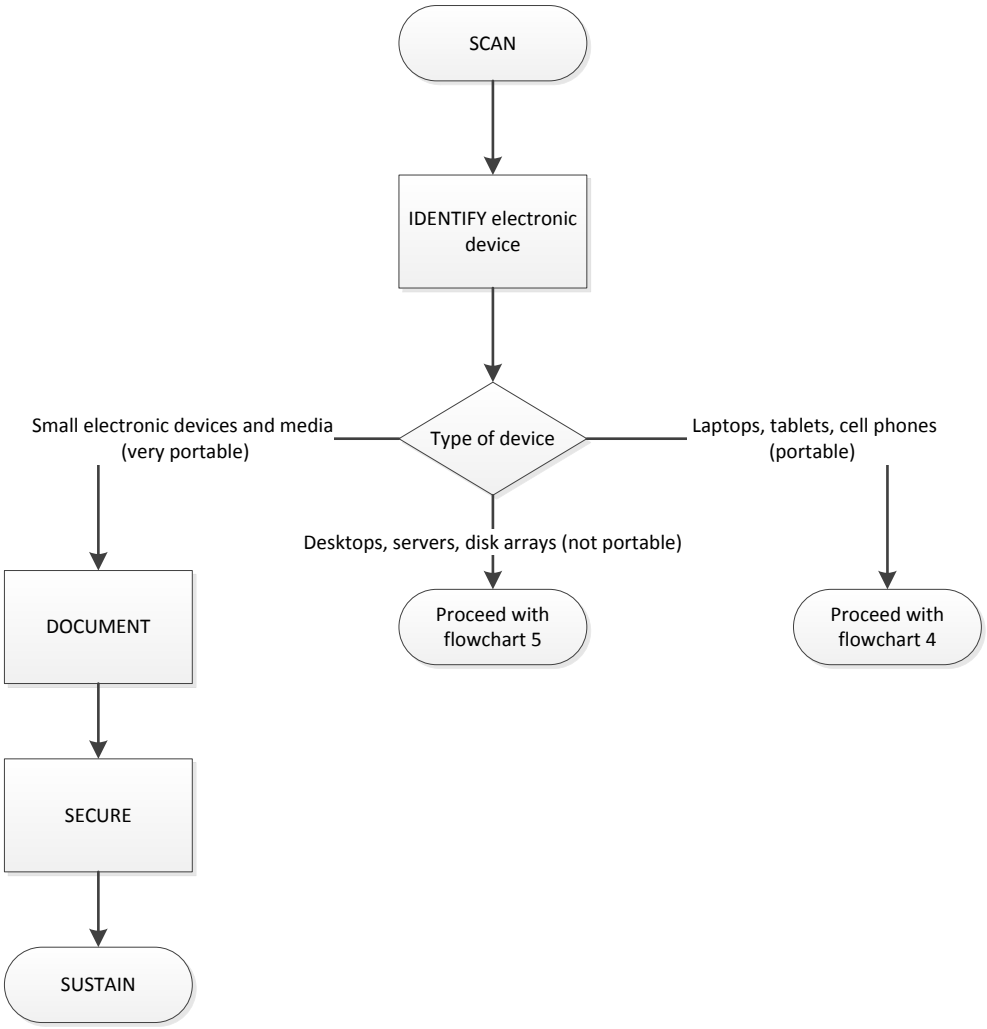
8 Exfiltration Solutions

Michal Sadlon

Exfiltration is one of the most difficult parts of the forensics process and covers activities over the entire triaging model. Exfiltration does not only consist of acquisition: there are also other important operations that should be done throughout. As mentioned in Chapter 6 – 'Computer Forensics', there are several aspects leading to different scenarios.

8.1 Exfiltration Process

Flowchart 3 depicts the exfiltration process by including all steps of the SIDSS triaging model. Scenarios mainly depend on the type of electronic device being identified. Therefore, the identification phase is important.



Flowchart 3. Exfiltration process.

Device type/size: (see Flowchart 3) the following types have been recognised:

·VERY PORTABLE: small electronic devices and removable media (USB media, CD/DVD, external hard disk, camera, audio recorder, SIM cards ...).

·PORTABLE laptops, tablets, smartphones, cell phones, game consoles, GPS devices, smartwatches and other portable devices that have their own operating system able to communicate or connect over the network or Internet.

·NON-PORTABLE desktops, servers, disk array or RAID solutions or network device/appliance.

In addition to the above, any of the following may be important to collect for later evaluation:

- handwritten notes
- personal organisers, desk or personal calendars, address books
- potential usernames, passwords, e-mail addresses, web sites and IP addresses written on scraps of paper in the strike area

8.2 Very Portable Media and Electronic Devices Collection

The first category from Flowchart 3 includes different types of small electronic devices that may store data in digital form and are easily portable. Examples are media cards (SD, SIM, flash), USB thumb drives, optical media (CD, DVD, Blu-ray), digital cameras, MP3 players, external hard drives, tape and cartridge storage.[32] The unique thing about these types of removable media is that the information written to them is not lost or deleted when the power to them is disconnected.

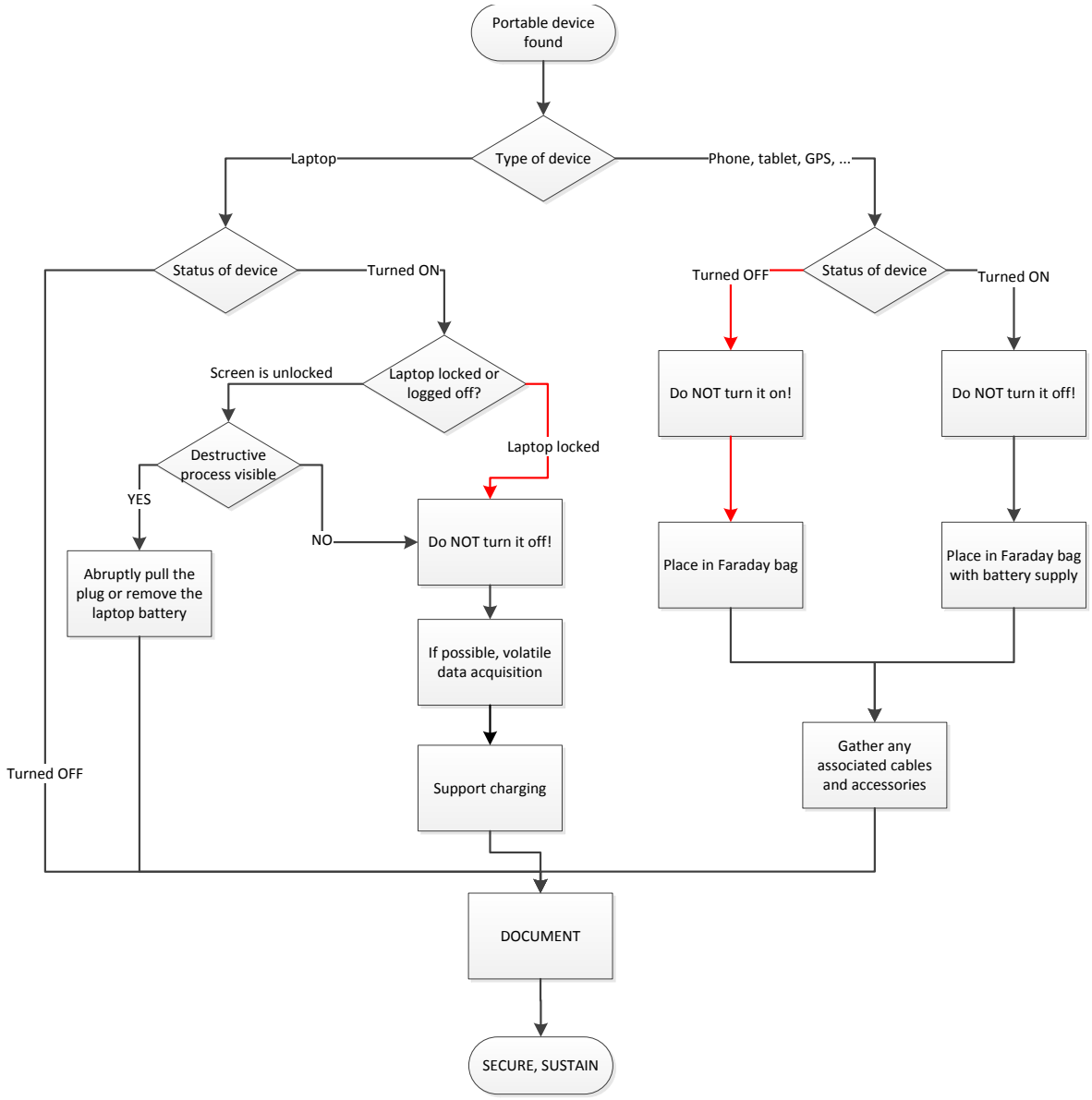
Devices from this category are usually small devices and may not always be available in the information processing device or in its vicinity. They are often retained by the user or are stored off-site, and may be overlooked in the identification phase if they are not immediately identified. As technology changes, there will be newer and different types of removable media and it is essential that SOF operators keep up-to-date with this changing area.

Their collection consists of documenting the devices (photograph or video) and proper packing into paper evidence bags or anti-static evidence bags. Be careful not to scratch optical media during seizure.

8.3 Portable Devices Collection

Flowchart 4 shows the process of collecting portable devices. These devices are able to store, process and transfer digital data. This category includes laptops, tablets and different types of mobile devices such as smartphones, cell phones, PDA, GPS devices, smartwatch, etc.

[32] Be aware also of legacy media such as floppy disks.



Flowchart 4. Portable devices collection process.

If the found device is a laptop, the SOF operator must check if the device is turned on or off. The power state can be determined as follows [27]:

- check for any LEDs showing activity;
- check for disks spinning;
- check for fan running;
- other signs of activity (feel for heat or vibrations, ...);
- check whether any connected output or input devices show any activity.

Make sure that the laptop is switched off – some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine is switched on [28]. Be aware that some laptop computers may power on by opening the lid.

If the system is off, do not turn it on! If possible, remove the battery from the device and prepare it for transportation (package the device using a bag).

Figure 14. How to remove battery from a laptop (example).[33]

If the system is on, do not type or click the mouse. If the screen is blank or a screen saver is present, a short movement of the mouse or touchpad should restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video record it. If the operating system is not locked or a user is logged in, try to execute volatile data acquisition. The volatile data or memory dump collection process has to be automatised as much as possible, to avoid any reaction delay in the operation. If the OS is not locked or the user is logged in, and it is possible to see from the screen that destructive processes[34] are running, the power cord or battery should be removed from the back of the computer and connected devices. This is an exception to the procedure for powered on systems. More information about destructive processes can be found in Chapter 7 – 'Anti-Forensics Measures'. If the system is on but the screen is locked, check the presence of a FireWire port on the device (see Figure 15). With the right equipment,[35] it is possible to acquire the content of the RAM by using Direct Memory Access (DMA).[36] Finally, support a charging of the laptop and prepare it for transportation.

Figure 15. a) Firewire port on the laptop (port in the middle) [29] and b) two Firewire ports [30].

[33] Figure f*rom http://www.computerhowtoguide.com/2011/09/how-to-take-care-of-your-laptop-battery.html*

[34] Destructive processes can be any functions intended for example to wipe evidence from storage media. Terms like 'format', 'delete', 'remove', and 'wipe' can be indicators of destructive processes [31]. However, these may be in a foreign language.

[35] One example tool is CaptureGUARD Gateway, provided by Windows Scope [32], which allows access to locked Windows computers.

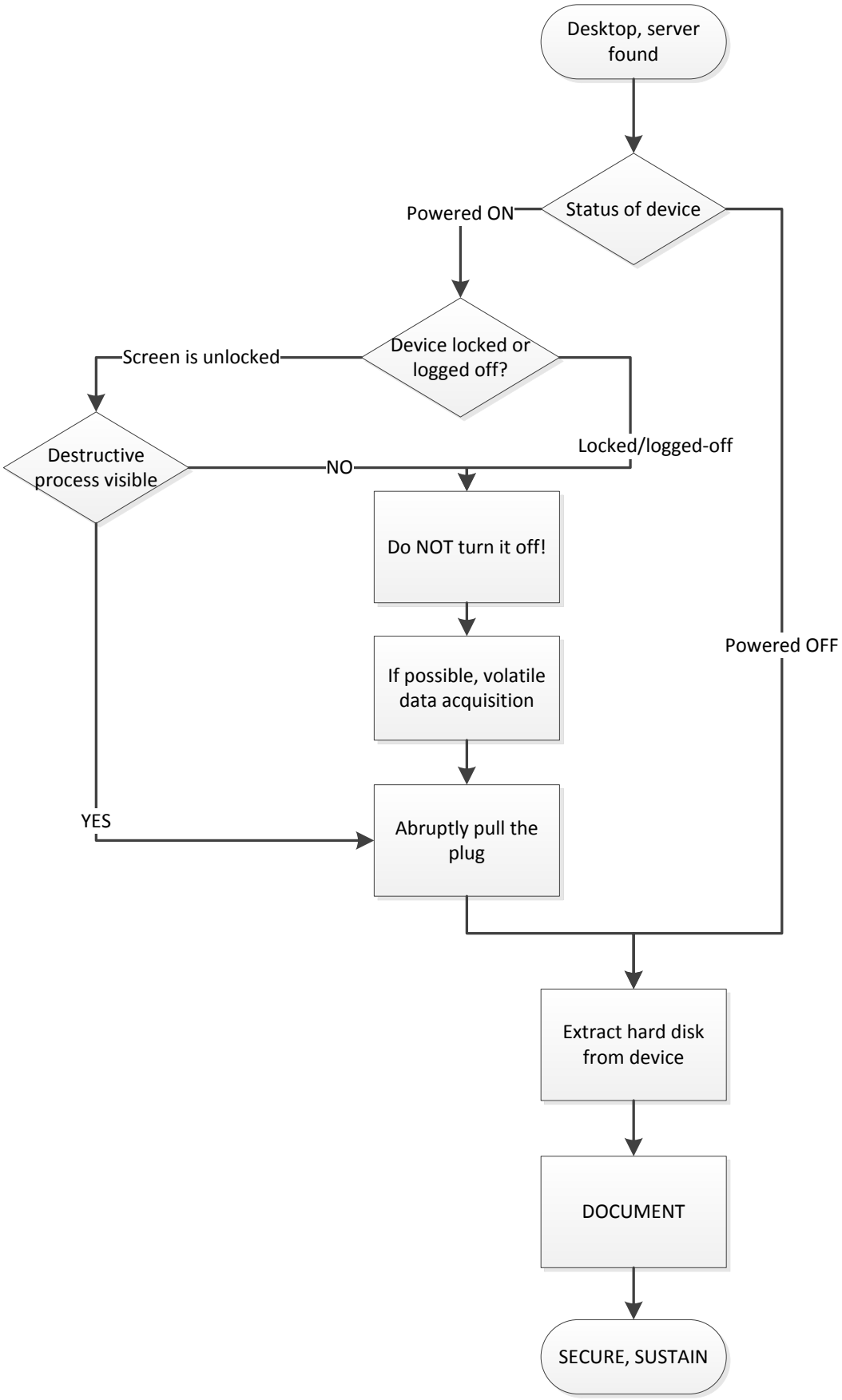
[36] FireWire interface is an example high-speed expansion port providing an option for a DMA attack [33]. An example open source library for performing memory forensics over that interface can be found from GitHub [34].

As with other portable devices (such as phone, tablet, or GPS), the first task is again to determine if the device is on or off. Helpful steps are: look for lights, listen for sounds, feel for vibrations or heat. Many mobile devices save power by turning off screens after a specified amount of time [28]. Despite the screen status, the device is likely still active: pressing the home button quickly will activate the screen.

If a mobile device is off, do not turn it on! Depending on the device type, it is possible to remotely manipulate them, including deleting all stored information. Therefore, pack the device into a Faraday bag. If the device is on, do not turn it off. Place it in a Faraday bag but support charging with a portable battery charger (both device and charger should be inserted in the bag). Look for and gather any related accessory, for example cables, PIN codes, or security unlock information.

8.4 Non-Portable Devices Collection

Flowchart 5 describes the process of gathering information from devices that are non-portable, mostly because of their size. Examples are desktop computers and servers. In some cases, the amount of data that has to be processed will preclude on-site collection. There are a number of different operating systems and hardware specifications that may be encountered, and this impacts on-site digital forensics activities.



Flowchart 5. Non-portable devices collection process.

Devices might be found in different states:

- device is discovered in power-on state
  - unlocked (direct access to device)
  - locked/user logged-off/…
  - in suspend mode[37]
- device is discovered in power-off state

If the computer system (desktop, server) is powered on, the SOF operator should try to acquire volatile content. Volatile evidence may help the investigation or it might be the only evidence there is! If it is not taken, this will undermine the digital evidence investigation. The importance of acquiring this data is covered in paragraph 6.3 – 'Assessing Gatherable Intelligence'. This part of the exfiltration process makes demands on the technical architecture supporting the SOF team (See paragraph 6.2.1.3 – 'Vector Options'). The technology used has to follow the order of volatility. The huge variety of possible devices and operating systems means that it will be a challenge to prepare a convenient exfiltration point capable of gathering not only RAM dump, but also options like temporary system files, swap files, network configuration and settings if available. [28, chapter 8.6.18.2]

Devices in this category may also contain a FireWire port. Check if a port is available, to use it for RAM acquisition.

The next step after the volatile data acquisition (if the system is powered on) is to shut down the device. It is recommended to do this abruptly by removing the power (the 'pull the plug approach').[38] This action must also be taken if any destructive operation is visibly running on the system. The following step is the physical extraction of the storage from the device. A spinning hard disk or solid state disk (SSD) may usually be found inside current desktop computers

Physical extraction consists of extracting media devices that are parts of a physically bigger system (such as a desktop or server) and that are not easily transportable during the operation. It may result in removing different types of disk drives that are built into computer systems. Note that if a RAID 0 setup has been used (as an anti-forensics measure[39]), this requires discovering and extracting all the disks used in the setup.

a) Remove the hard drive (step-by-step instructions)

Note: This guide applies to a hard drive that is mounted inside the desktop computer case. A cordless electric screwdriver is usually needed to open the desktop (server) case and handle the drive if it is fixed.

1. Make sure the computer is powered off and the power cable is disconnected.

[37] In some devices it may be possible to detect the suspend mode from slowly blinking LED lights. For example, because of security bugs [35], it is possible to see the OS's desktop contents on resume from suspend before the lock dialog. For capturing the content from the screen in such a scenario during a special operation, a (high speed) video camera would be required. If the suspended device is properly secured into a Faraday bag with battery supply, this can be done after the special operation in the forensics investigation. This means that resuming should be tried during the secure operation only if it is not possible to capture the suspended device (for example because of the size of it).

[38] If a graceful shutdown is undertaken, then there may be data destruction (for example if the equipment has been booby-trapped) or other ways that the evidence may be altered during the graceful shutdown process.

[39] Read more from paragraph 7.1 – 'Data and Device Hiding'. Before removing devices it should also be remembered that hard disks and SSD drives may be encrypted.

2. Open the desktop computer case. Use a cordless screwdriver to increase the speed of opening the case, if the case is closed with fixed screws. Be aware of locks that prevent opening the case: if these are present, additional tools providing capability to cut metal might be needed.

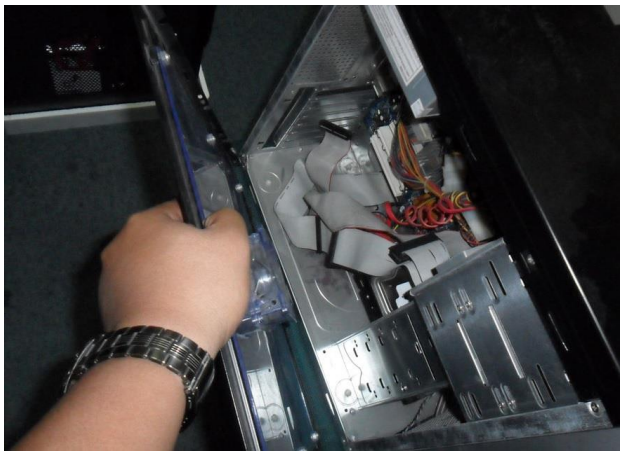


Figure 16. Locating computer's drive bay with the hard drive [36].

3. Locate the computer's drive bay with the hard drive, as shown in Figure 16. Check if there are any marks of hard drives and/or cables being removed many times, as they might be the result of a RAID-0 or other anti-forensics setup.

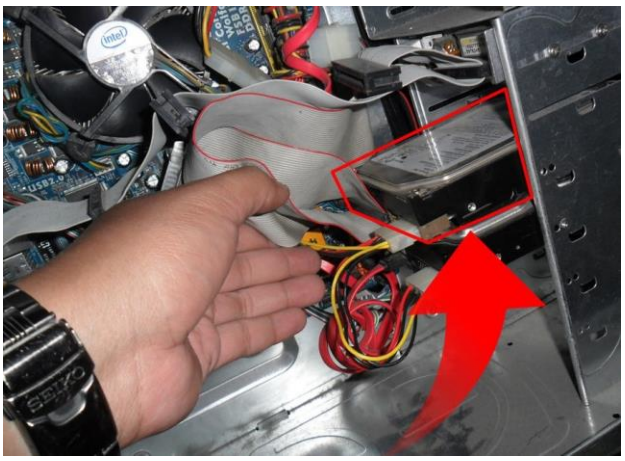


Figure 17. Removing the drive from the drive bay [36].

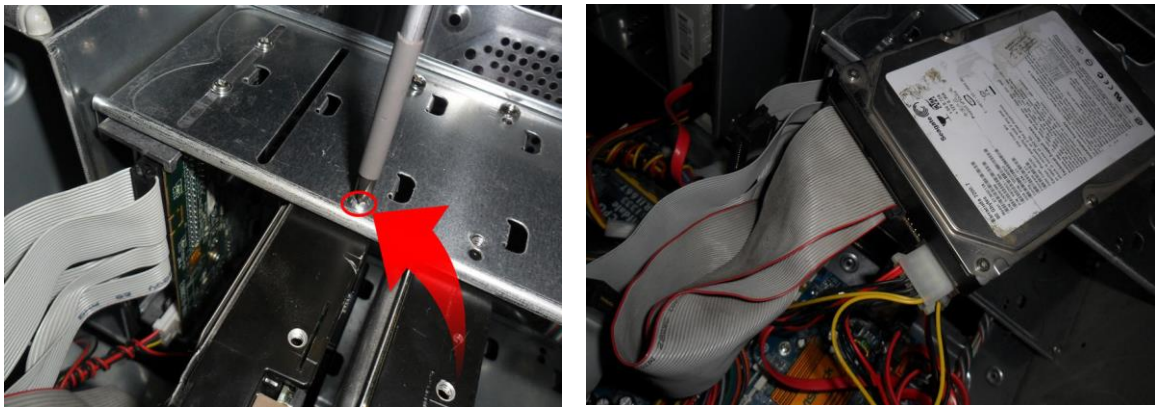


Figure 18. Removing the drive from the drive bay [36].

4. Remove the drive from the drive bay, as shown in Figure 17 and Figure 18. Note that sometimes it is easier to first remove the whole drive bay from the case, and then take the drives out of the removed drive bay.

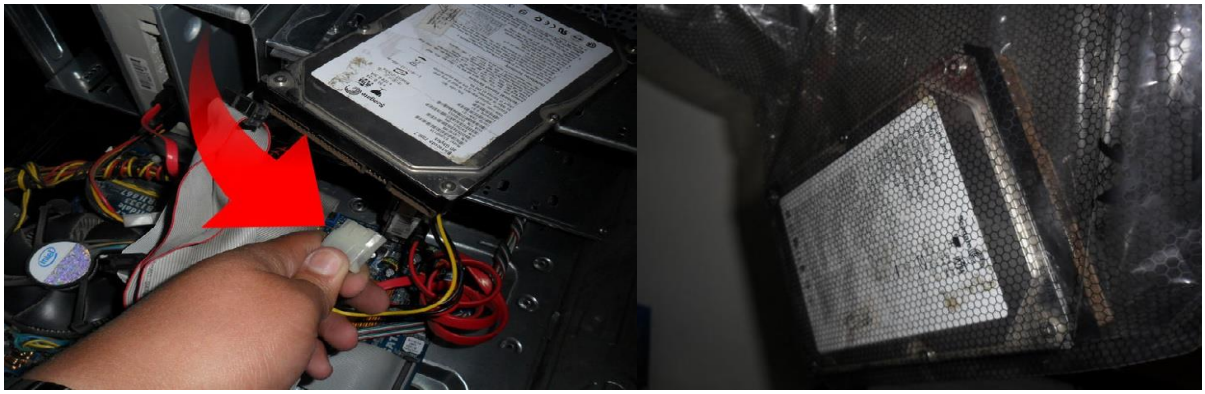


Figure 19. Unplugging data cable and power cable [36].

5. Unplug the data cable and remove the power cable from the hard drive. This is shown in Figure 19. Document drives which are missing some or all required cables, as they may be part of anti-forensics setup using for example RAID-0.

b) Remove the SSD disk (step-by-step instructions).

Note: This guide applies to most SSDs. A cordless electric screwdriver is usually needed to open the desktop (server) case and handle the drive if it is fixed.

1. Make sure the computer is powered off and the power cable is disconnected.

2. Open the desktop computer case.

3. Locate the computer's drive bay with the SSD drive.

Figure 20. Unplugging the SATA data cable and SATA power cable from the SSD[40] drive [37].

4. Unplug the SATA data cable and SATA power cable from the SSD drive, as in Figure 20.

[40] Original photo by Simon Wüllhorst https://www.flickr.com/photos/descilla/3377031204.

5. Remove the drive from the drive bay with care. Follow the safety notes:[41]

- Handle the SSD with care, keep it in the protective anti-static sleeve
- Do not touch connectors on the SSD drive
- To minimise static electricity, touch the desktop case before handling the SSD.

8.5 Equipment and Tools Required

The following equipment and tools are needed:

- Portable battery chargers
- Antistatic bags, antistatic bubble wrap, Faraday bags/boxes, cable ties, evidence bags, evidence tape, packing materials (avoid materials that can produce static electricity), markers
- Pliers, electric screwdrivers with various heads.

8.6 Document Phase

8.6.1 Photographing/Recording the Scene

Photographing or video recording[42] is the crucial part of the *document* phase. It should be the first step taken by the SOF operator on arrival (together with the *scan* phase). This will also accurately depict the condition of the scene prior to any evidence collection or disruption that will probably happen during processing [28].

Ideally, video recording goes from the overall scene down to the smallest pieces of the evidence. As mentioned before in this chapter, do not forget to record the status of the monitor screen.[43] Photographs or video should also be taken of the rear of information processing equipment, to accurately display how the cables are connected. It is helpful even if the equipment is not to be seized: as it is present, it should be recorded.

As described in paragraph 10.3 – 'Documentation of Evidence', photographing and recording the scene are important. Cameras providing a 360° picture could be helpful, not only for documenting the scene, but also for scanning and identifying devices. If a convenient video streaming can be originated[44] from the tactical site towards the tactical operations centre (TOC), forensics experts can remotely advice SOF operators. The video streaming should also prevent any form of operators' identification by using blurring techniques, as explained in Chapter 10 – 'Chain of Custody.

8.6.2 Packaging and Labelling

All evidence collected should be marked as exhibits so that they can be easily identified at a later date [39]. All exhibits must be properly seized, labelled, transported, and handled for evidence recovery purposes. The labelling or marking of the evidence begins the chain of custody of the items of evidence (see Chapter 10 – 'Chain of Custody'). The label should contain at least the following information [38]: description of the item, date, location of collection, operator name or identifier, and brand name. The labels must be affixed to all

[41] SanDisk [40] provides an installation guide with safety notes for handling SSD drives.

[42] It should be completed prior to any evidence seizure but within the short timeframe of the SOF strike it can be done parallel [28].

[43] If a screen saver is being used, press the down arrow key to redisplay the open file or the password-protected login screen.

[44] Chapter 9 – 'Sustaining the Data' covers techniques to create communication channels; yet convenient bandwidth for high quality video streaming is a challenging requirement, so most likely only 360° images can be provided.

items of the evidence, typically on the dedicated evidence bag.[45] Since the operation will be executed in an extremely limited timeframe and likely in a hostile environment, labelling should be done as soon as possible in a friendly environment.

Evidence must be packaged in a way that it cannot become damaged (moisture, dust, vibration). Appropriate evidence bags should be used for the different types and sizes. The use of Faraday bags or boxes is recommended if it is necessary to isolate devices that use wireless communications (PDAs, cell phones, etc.). In general, it is important that computers or other electronic equipment or media are handled gently. Bubble wrap can be used if available, to minimise or absorb vibrations.

Packed evidence must be protected from any sources of magnetism or similar sources of power that could negatively affect the integrity of some electronic evidence.

[45] Evidence bags may be pre-printed or evidence tags made to be affixed to the exhibits.

9 Sustaining the Data

Hayretdin Bahşi

In the limited time-frame of an operation, SOF operators may not have the opportunity to collect all the devices. One alternative way of obtaining information from the devices may be to install surveillance software on the target devices and set up an information channel based on the existing internet connection or a network which can be swiftly established in the theatre during the operation. This information channel may enable collection of the data to begin during the operation. The collection phase may even continue after the completion of the mission, depending on the survivability of the channel.

In this chapter, existing technology and research projects are investigated for the preliminary analysis of gaps between current technology and the solutions required specifically for battlefield digital forensics. Using an existing internet connection for data extraction is a widely known scenario which can be executed using existing tools and technology. Thus, this chapter does not cover detailed discussion of data exfiltration via the internet, but focuses on establishing an additional network infrastructure.

In cases where an internet connection is not available, SOF operators may apply two approaches for data collection. The first approach is to establish a temporary wireless local area network (WLAN) in the site area and place a data collection server in this network, which remains in the area only during the operation. The data collector server acts as the computer that stores the obtained digital forensics data. A helicopter can be included in the WLAN so that it can host the data collector, which eliminates the need for carrying an additional device. In this approach, all the network components are removed from the site after the completion of the mission, which means that collection of the forensics data is only enabled during the operation time. However, the local area network may provide a high data transfer rate.

The second approach is to establish a connection to a satellite or a drone (UAV) from the theatre, which will still remain after the operation. In this approach, the forensics data is transferred with lower data transfer rates, but the connection continues until the related network devices run out of battery or the enemy destroys the connection infrastructure. If the position of the UAV enables it to be part of a WLAN, higher data transfer rates may be possible. The data collector can be located in a secured site, which can be accessible over satellite or UAV; it may even be integral to the UAV itself. The main drawback of this approach is that it requires leaving network devices in the theatre after the operation, which may cause higher operation costs or create room for the enemy to carry out forensics analysis on the devices and conduct cyber-attacks against the data collector.

Regardless of the alternative chosen, the relevant network infrastructure should be designed according to the inherent limits of operations. The first requirement is that the devices of this network should be easily deployable and require only a small amount of configuration during the setup. This configuration should be possible for non-technical people to do in a short time. Secondly, all the installation equipment and network devices should be portable and should not exceed the carriage limits. Thirdly, network devices with lower energy consumption and higher bandwidth capacities are preferable in order to increase the amount of forensics data that can be obtained from the site. Lastly, environmental and structural factors such as the existence of walls and signal blocking materials, and the weather situation, should be carefully considered during the network establishment phase.

The analysis given in this chapter focuses on establishing wireless networks due to their easy deployment. Therefore, digital devices which already have wireless interfaces can be chosen as targets for the data extraction. The SOF operators may also insert wireless USB adapters to the relevant targets that have no wireless interfaces.

9.1 Surveillance Software Installation and Forensics Data Extraction

There are commercially available surveillance software tools[46] that are used by law enforcement bodies for the purpose of tracking criminal suspects. These tools place malware on the suspect's computer using various methods such as compromising vulnerabilities in popular software, using flaws in their update mechanisms or installing malicious code with spear-phishing e-mails. Removable storage devices like USBs can easily be used for the same purpose. The malware enables the law enforcement body to control the suspect's computer remotely, obtain important files and credential information, and intercept the suspect's communications.

In the battlefield forensics scenario, surveillance software can be used to extract forensics data during and after the operation. As SOF operators can physically access digital devices, they can install this software through USBs or similar removable media. The main function of the installed software is to find and extract relevant data on the target device and send them automatically to the data collector server. It may seek internet connectivity and then send the forensics data to the data collector server over the internet. If there is no existing internet connection, the software can use a network connection established during the operation by the SOF operators.

The inherent nature of the target infrastructure puts many technical and operational restrictions on the duration of the connection and the amount of data that can be obtained. Therefore, the data extraction strategy should rely on searching the data for specific content rather than obtaining the whole image of the target device. Equipping the surveillance software with the relevant search patterns can be a vital forensics preparation step for the operation. Search patterns may include user credential data, as this data may be useful for the analysis of other digital devices directly collected from the site or it may enable further cyber operations to be conducted against other enemy information systems.

Digital devices for surveillance software installation can be selected according to intelligence available before the operation or decisions made by SOF operators during the operation. Operators may prefer to install malware in the computers which weigh more than the carriage limits and those which may be assumed to have critical information.

9.2 An Optimised E-Discovery Tool

In recent years, e-discovery forensics tools[47] have been developed which allow transferring selected files, system and other forensics-related data from remote computers to a central server; these are used to help the IT and legal departments of businesses. These tools require the installation of software agents in the remote computers. Rather than conducting analysis of the data, the aim of the software agent is to transmit the selected data to the central server over the existing network infrastructure. Under the extreme conditions of the SOF strike, forming a communication channel by installing surveillance software can be combined with the rapid installation of an e-discovery solution. Quick and automatic installation of the software agent in the target computer is essential. This agent should be able to carry out possible network configurations before sending the data; it should include the relevant search patterns and should be able to optimise the length of search results and even erase itself after the completion of the mission. Once the relevant network infrastructure is established in the site area, an optimised e-discovery tool can be the solution for sustaining the forensics data.

---

[46] One commercial tool is FinFisher: https://www.finfisher.com/FinFisher/products_and_services.html

[47] Examples of e-discovery tools are AccessData's AD eDiscovery http://accessdata.com/solutions/e-discovery/ADeDiscovery and Guidance Software's EnCase eDiscovery https://www.guidancesoftware.com/encase-ediscovery.

9.3 Establishing a Temporary Wireless Local Area Network

The temporary WLAN alternative aims to collect forensics data during the operation, from digital devices that have wireless network interfaces and by taking advantage of high-speed local area network connections. Since the data collector server is carried to the target site or located in a helicopter, there is no need for an external connection from the WLAN to the internet or another wide area network. A portable wireless access point and several mesh network repeaters can form a temporary IEEE 802.11 WLAN.

The data transfer rates may change according to the number of hops, the distance from the access point, the existence of physical obstructions such as walls and signal blocking materials, the number of clients, the capacity of the wireless adapter of the target digital device and other environmental conditions. The coverage area of the WLAN also depends on the physical and environmental conditions.

Significant preparation activities before the operation will be the collection and analysis of intelligence about the physical attributes of the site, possible locations of digital devices and weather conditions at the planned operation time. The SOF operators should plan how to setup the topology of the temporary WLAN according to the estimated ITTI complexity. Plans should include determining the exact locations of the access points, repeaters, power supply sources and other network devices.

Various indoor or outdoor high performance access points are available on the market. For example, an indoor access point can have a network performance of 1.734 Gbps data rate in 5Ghz frequency with 802.11ac.[48] MAC Efficiency rate is assumed to be %60 in some benchmark studies.[49] If it is assumed that the maximum output rate given in the product specification is reached with %60 MAC Efficiency rate, a ten-minute operation may enable the transfer of up to 78 GB of forensics data. The wireless signal coverage of this access point can be extended up to 465 m^2. The size of coverage area can be considered as reasonable for the studied case as the whole site can be covered by additional mesh repeaters if needed. Outdoor access points can establish up to 20 km of point-to-point links using high-gain antennas[50]. A combination of indoor or outdoor access points can be used to establish wireless mesh network according to the physical properties of the site.

The performance of the data collector server should allow the capture of all the network traffic coming from the digital devices. Wireless adapters are available with speeds up to 2100 Mbps in 5GHz band.[51] The hardware of the server should enable the forensics data to be filtered from captured traffic and written to the storage at high speed. The data collector server should be portable and include an appropriate size of battery.

Access points can include built-in USB interfaces. This means that the same access point can act as a data collection server if a relevant data storage unit is integrated through this interface. As USB 3.0 can provide data rates of up to 5Gbps, writing the data to storage may not create an additional burden on the performance of data collection if the access point can process the incoming data at high speed.

9.4 Access to Satellite

A communication channel from the site to a data collector server located in the secure area can be established over a wide area network. If the target digital device has an internet connection, the surveillance software just uses it for sending the forensics data.

---

[48] https://www.asus.com/us/Networking/RTAC87U/

[49] http://www.cisco.com/assets/global/CZ/events/2015/ciscoconnect/pdf/TECH-MOB-1-Novinky-JaroslavCizek.pdf

[50] https://meraki.cisco.com/lib/pdf/meraki_datasheet_MR72.pdf

[51] https://www.asus.com/Networking/PCE-AC88/

A communication channel to satellite can be set up over portable Wi-Fi internet hotspots, which establish WLAN in the target area and create a connection to satellite from this network.[52] These devices can provide 350-500 kbit/s internet access over satellite links, and can be deployed in less than a minute; they weigh nearly 11 kg meaning they can be carried by SOF operators. If the target digital device has a wireless network interface, it can be configured to access the internet over these hotspot points by the surveillance software installed during the operation. The hotspot can create a wireless area within a range of 100 meters. Its internal battery can run for up to 5 hours, which means that in case of having no external power supply, the communication channel is still able to obtain approximately 1 GB of data even if the MAC efficiency is not taken into consideration. The location of the hotspot should be carefully chosen, as it requires to be on the surface with a clear view of the sky and within 100 metres of the target digital device. If both conditions cannot be satisfied due to a long distance from the digital device, repeater devices can be used between the hotspot and the location. Foldable solar panels can be used for recharging the battery, which may help to collect much more data after the end of the mission.

A cheaper alternative to providing internet access can be the use of satellite phones as internet hotspots.[53] However, the low data transmission rates, such as 2.5 Kbps, make this alternative impractical for battlefield digital forensics purposes.

9.5 Access to UAVs and Other Aerial Vehicles

An aerial vehicle located near the target site may act as a gateway to a satellite or it can itself host the data collector server. Depending on the offensive capabilities of the enemy, this vehicle may continue to operate or may move away from the site after the completion of the mission. In most cases, its level of security may be correlated with its operating altitude, with higher altitudes meaning better security. On the other hand, as the targeted area encompasses a relatively small extension such as several square kilometres, the functional requirements do not require operating at higher altitudes. Additionally, lower altitudes may enable data transfers with higher rates, thus obtaining more forensics data. Based on the altitude, the vehicles are categorised into two groups: high altitude platforms and low altitude platforms.

High altitude platforms: aeroplanes, balloons or airships, operate between 20 and 50 km. The Northrop Grumman RQ-4 Global Hawk UAV is an important and widely known example of a high altitude platform.

Google's Project Loon has air balloons travelling approximately 20 km above the Earth's surface in the stratosphere. Project Loon uses software to determine where its balloons need to go, and to move the balloons into the correct layer in the stratosphere to be moved with the wind to the desired locations. Electronics in the balloons are powered by solar panels. Each balloon can provide connectivity to a ground area about 80 km in diameter using LTE. The balloons relay traffic from LTE-enabled devices such as cell phones back to the global internet. The project's pilot test phase started in June 2013 [41].

It is uncertain if in the future it will be possible to rent the Project Loon communication networks from Google, for example to provide LTE connectivity for specific areas. If not, there is also balloon-based communication provided for the military. Space Data provides SkySat, which is a balloon-based repeater platform. Balloons are also working in the stratosphere;[54] it is claimed they extend the range of standard-issued military two-way

[52] http://www.groundcontrol.com/MCD-4800_BGAN_Terminal.htm

[53] http://www.groundcontrol.com/Satellite_Phones.htm

[54] There are also examples of using air balloons a lot closer to Earth: based on [42], in 2013 Oceus Networks [43] applied for permission to demonstrate a LTE-based tactical communication system for the US Army, in which air balloons were tethered only 650 meters from the ground. The shorter the distance between balloons and LTE-enabled devices, the more bandwidth can be used. However, if the air balloons can be easily seen by the enemy, various risks arise, such as shooting them down.

radios from 10 miles to over 500 miles.[55] SkySat FM was employed as a military platform in 2007 and has since been used in various missions. Unlike Google's Project Loon, SkySat does not use solar panels but the battery life is 8-12 hours. [44]

ABSOLUTE (Aerial Base Station with Opportunistic Links for Unattended and Temporary Events) is a FP7 European research project that provides a high-capacity IP mobile data network for public safety and tactical applications.[56] The project covers the deployment options of aerial base stations, portable land units and user equipment in a land-and-air-based communication architecture that finally maintains connectivity between ground and satellite. The system architecture of ABSOLUTE is shown in Figure 21. Aerial eNodeB (AeNB) is the aerial base station that provides Ka-band communication between ground and satellite. In this architecture, this base station is located on a low-altitude platform, which is a helium inflatable kite. Drone small cells (DSCs) which act as aerial wireless base stations can be placed on UAVs in order to provide wireless services [45]. In ABSOLUTE, AeNBs need to be transported by truck; additional time and effort is required for their deployment which means they may not be easily utilised in our battlefield digital forensics case. However, the DSC alternative can be chosen due to its easy and rapid deployment capability. It can be also a viable solution if the operation is already supported by UAVs for other purposes.

ABSOLUTE also includes a terrestrial communication platform, Portable Land Mobile Unit (PLMU), which can be placed in harsh terrains where AeNBs cannot be deployed. They can be also used with AeNBs in order to increase the bandwidth availability. The PLMU integrates a Wireless LAN router and a Ka-band satellite modem. In the battlefield scenario, they can be deployed in a helicopter or in the site area theatre to provide the link between satellite and ground. Via the Wireless LAN router, they can collect the obtained forensics data and relay to other points.

In the study's battlefield case, UAV integrated versions of AeNBs or PLMUs can relay the forensics data obtained from the target site to the network endpoint in a closer secure area, or they may transmit them to distant locations via satellite links. Rather than doing the relaying function, AeNBs can also store the forensics data themselves.

[55] It is claimed that the system provides connectivity even into deep canyons and valleys.

[56] http://www.absolute-project.eu/images/ABSOLUTE_white_paper_2015.pdf

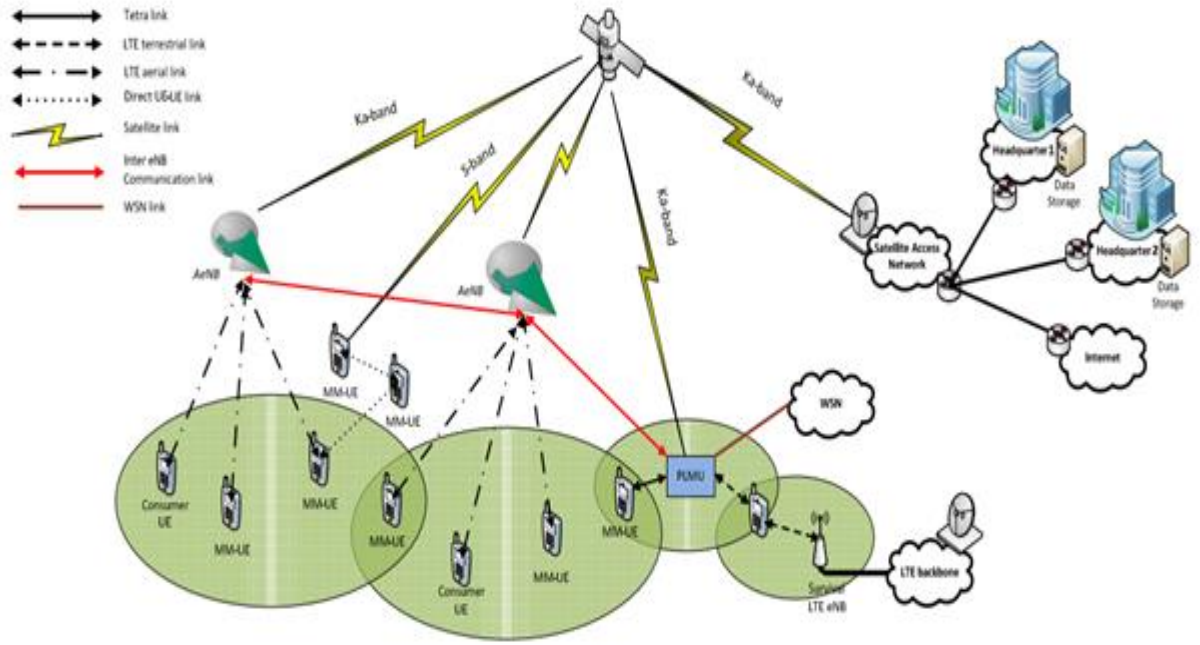


Figure 21. ABSOLUTE System Architecture.

9.6 Establishing Wireless Sensor Networks

Wireless sensor networks (WSNs) are widely deployed for monitoring purposes in applications such as health-care, industrial or environmental monitoring. One example WSN that could be used to monitor environments in military operations is Smart Dust. It contains small sensors that are the size of dust particles (1-2 mm), as shown in Figure 22. Despite their small size, the sensors have computing capabilities and can be embedded into power supply equipment for two-way wireless transmission and solar electricity functions. In military operations, these sensor particles can be distributed over an area of interest to acquire real-time data. As mentioned by Kahn, Katz, and Pister in [46], considering the military arena, Smart Dust may be deployed for stealthy monitoring of a hostile environment, for example for verification of treaty compliance. It could also be used for perimeter surveillance, or to detect the presence of chemical or biological agents on a battlefield. In addition, it is possible to trace individuals with precise information of time and location. Sensors are able to measure among other things, acoustics, vibration, magnetic field, temperature, humidity, acceleration and pressure[57] [47][48].

[57] Acoustic, vibration or magnetic field sensors could detect the passage of vehicles and other equipment [46].

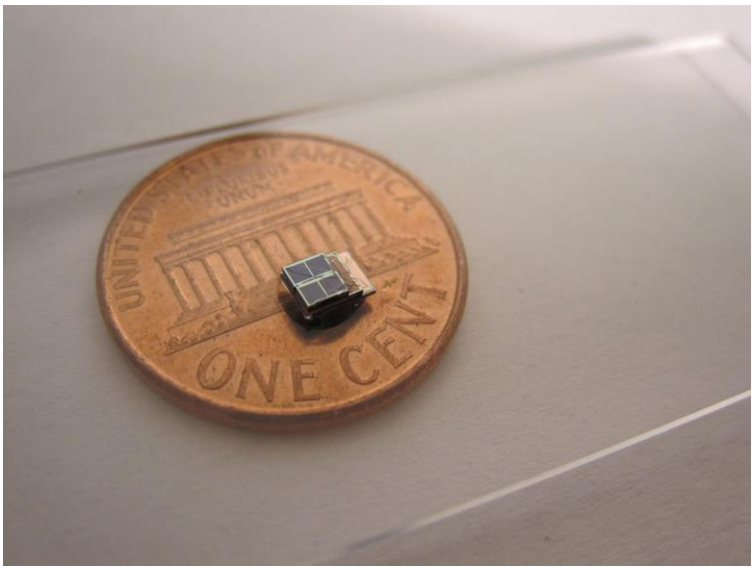


Figure 22. Smart Dust sensor[58].

In addition to collecting information before the special operation, they could be used to transfer, at least, small amounts of captured data out from the target site. WSNs are useful in simple monitoring applications requiring low data transfer rates. They operate with low power consumption in order to prolong the monitoring function as much as possible. Although there are efforts to increase the data transfer rates, these rates do not exceed 2 Mbps [49]. In the battlefield digital forensics case of this study, as the area is not very wide and the SOF operators can locate network devices with appropriate batteries during the operation, establishing IEEE 802.11 WLAN with high data transfer rates is more feasible. It can be argued that WSNs can continue to operate after the completion of the mission and would be able to transfer data for a long time due to their low power consumption. However, as the area belongs to the enemy and the SOF operators only have control of the area for a limited time, it is highly probable that the enemy would find and destroy the network infrastructure within a short time after the operation. The characteristics of the operational environment thus do not allow WSNs to use their advantage of low power consumption.

9.7 General Overview of Alternatives

Based on the already existing communication technologies, it may be possible to setup a system (or several systems) for transferring data out from the target site during and after the operation. As discussed, establishing a temporary WLAN only enables data to be collected during the operation. The creation of a communication channel via satellite which can remain after the operation has been described as an alternative to a temporary WLAN; however, the temporary WLAN enables the collection of much more data due to the high data transfer rates provided by local area networks. Moreover, all the devices of the network infrastructure can be removed from the theatre during the operation, which may be significant for covert operations. Although both alternatives enable some amount of forensics data to be obtained from the site, even the best alternative cannot transfer all the data from an ordinary user computer. Therefore, determining specific search patterns and finding the relevant data in the digital devices is vital in this case of study.

[58] *Photo by Daeyeon Kim: http://ns.umich.edu/new/releases/7520.*

10 Chain of Custody

Kris van der Meij and Mario Huis in 't veld

10.1 Legal Framework for Operations

The *jus ad bellum* recognises three generally accepted legal bases for the use of force by states:

1. The right to individual or collective self-defence, recognised in Article 51 of the UN Charter.
2. Authorisation by the UN Security Council based on the UN Charter (Chapter VI or VII).
3. An invitation from the host nation.

The legal framework that applies during deployment can differ for each operation, and even sometimes for different areas or phases of the same operation.

International Humanitarian Law (hereinafter IHL), *jus in bello,* as set forth in (inter alia) the Geneva Conventions and the associated Additional Protocols, governs conduct during armed conflicts, including SOF operations in that context. IHL only applies officially ('*de jure*') in situations of 'armed conflict', however, even when IHL does not apply officially, the majority of nations, including the NATO member states, apply the protective provisions of IHL in their policy as a safety margin for all military operations carried out by the armed forces. Next to IHL, International Human Rights Law (IHRL) applies[59] at all times and also during an armed conflict [50]. Neither are not limited by territory, they will apply wherever military operations are executed. [50]

Rules of Engagement (ROE) are rules or directives to military forces (including individuals) that define the circumstances, conditions, degree, and manner in which the use of force, or actions which might be construed as provocative, may be applied [52]. They provide authorisation for and/or limits on, among other things, the use of force, the positioning and posturing of forces, and the employment of certain specific capabilities. In some nations, ROE have the status of guidance for military forces; in other nations, ROE are lawful commands [53]. ROE are dependent on the mandate or legal basis for the operation. On the basis of national policy or national law, a state may impose restrictions on the agreed ROE and issue such restrictions to the deployed forces as supplementary instructions.

Troops will be deployed under a Status of Forces Agreement (SOFA), an agreement between states that generally establishes the legal framework under which military personnel operate in a foreign country. A Memorandum of Understanding (MOU) between the sending state and the host nation may contain additional agreements or guidelines on competence of troops in law enforcement operations.

10.2 SOF Operations

Operations, including SOF operations, will be executed in different circumstances, from relatively low-intensity peace support operations to combat operations. In most SOF operations, the available time for execution will be limited. In all circumstances, operations will be executed within the legal boundaries set by the applicable international and national law and reflected in the ROE.

Operators will be confronted with digital equipment, whether during a general operation or during a specific operation to collect information or evidence.

A. If the operation is executed to support criminal proceedings, the focus will be on the arrest of individuals and the collection of evidence for criminal cases in national or international courts. The

[59] Scholars and practitioners are not able to agree on how it applies [51].

collection of the evidence should be done according to the criminal proceedings law of the nation that will prosecute the suspect, or according to the rules of evidence of the International Criminal Court (ICC) [54]. Prosecutors, Force Provost Marshall (PM), Military Police (MP) and Legal Advisor (LEGAD) will be involved in the planning of this kind of operation.

B. When operators are confronted with digital equipment during an operation that is not intended to collect evidence for future criminal proceedings, the focus might be on collecting information for intelligence.

Proper documentation will be important in all operations, either to have evidence for a court case, to increase the value of the information for intelligence or, if applicable, to hand back the equipment to the lawful owner.

10.3 Documentation of Evidence

Accurate documentation of the obtained equipment or data is a prerequisite for successful criminal proceedings.[60] If the documentation fails or is insufficient, the collected equipment or data will likely not be admissible as evidence in court. Criminal law has strict rules on the use of evidence. Actions taken to secure and collect digital evidence should not affect the integrity of that evidence [55, pp. 13-15]. This can be achieved by following the procedures provided by the PM and MP during the planning of the operation. The use of proper tools (e.g. Faraday bag for mobile equipment, anti-static bags) is another prerequisite. Documentation can be done on the spot, but since the operation will be executed in an extremely limited timeframe and probably in a hostile environment, documentation should be completed as soon as possible in a friendly environment [56][57]. To conduct the documentation, the use of photo or video cameras (hand-held or mounted on helmet) is helpful and will increase the validity of the evidence. Operators should photograph/video/document the entire scene (360° of coverage, if possible). They should locate computer systems and electronic components/devices/equipment and determine how they are connected. Documentation should show the collection and sealing of the equipment before transportation. The photos and video captures should then be provided if requested by the prosecutor and/or the court. It is important for personal security that team members and Tactics, Techniques and Procedures (TTPs) are not recorded and if necessary these should be removed or blurred from the image. This removal or blurring has to be documented in an additional report, to avoid defendant claiming that the photos or captures have been manipulated. As well as the guidance provided by the PM and MP, procedures can be found in various documents [55, pp. 38-46].

Once documentation is finished, investigation will begin. There are strict procedures to follow in order to investigate equipment and data for criminal proceedings. It is recommended to have the equipment and data first accessed by law enforcement personnel (MP) before it is handed to the intelligence personnel, unless collection of information is the aim of the seizure. Specialised law enforcement personnel have the proper equipment and procedures to secure data for criminal proceedings without changing the data. If the strict procedures are not observed, the suspect might have a credible defence for court. Once the data or equipment has been examined by the MP, it can be released for intelligence.

10.4 'Illegal' Evidence

Even if the evidence is not collected according to the criminal proceedings law or may have been illegally obtained, it might still not be excluded from criminal proceedings.[61] There is a distinction between a citizen and

[60] Example of a documentation sheet can be found in Appendix F of Council of Europe's Electronic Evidence Guide [55].

[61] ICTY: The Prosecutor v. Radoslav Brdjanin - Case No. IT-99-36-T 'Decision on the Defence 'Objection to Intercept Evidence'' 3 October 2003, Trial Chamber II (Judges Agius [Presiding], Janu and Taya) [58]:

Admissibility of illegally obtained evidence – Exclusion of evidence under Rule 95 - Admission of intercept evidence and right to a fair trial.

police or other official investigators. The police, as a state actor, is bound by the criminal proceedings law, which aims to protect citizens against the power of the state. If the police have collected the evidence in violation of the law, this evidence will be excluded. If, on the other hand, the evidence is collected by a citizen, who is not restricted by the protection provided by this law, the evidence might be accepted. If the SOF operations are executed in support of law enforcement, it is reasonable to state that the operators are bound by the provisions set in the criminal proceedings law. However, the ICC accepts even illegally obtained evidence if there is no doubt as to the reliability of the evidence; otherwise the integrity of the proceedings is damaged.[62] Obviously, illegally obtained evidence will probably have less value in a court case.

If it is possible to collect data after the team has finished the operation, through the use of an existing or an established network (see: 6.4 – Sustaining the data), this data could be admissible as evidence for court, but there might be a need for a warrant to collect the data for an extended time. In any case, the collected data will be welcomed by the intelligence unit.

10.5 Responsibility for Obtained Evidence

Once equipment or data are obtained, the unit obtaining is responsible for this equipment or data until it's handed over to authorised personnel. Because the unit is conducting the operation under state responsibility, the state will be responsible for any shortfall in handling the equipment. This means, if the equipment, or data stored, gets lost or is accessible to third parties; the state will bear responsibility and will be liable for claims arising from the loss. This derives from the rule that in a criminal court case the judge will decide if the evidence will be returned to the legal owner, especially if the suspect is found not guilty. If data is copied and shared in the team, as one of the options to back up the evidence, it should be stored in such a way that no other parties will have access, e.g. by the use of encryption or techniques which will destroy the data in case of unauthorised access. Besides the possible liability in case of loss, the opponent would have the opportunity to identify which information has been captured and will take measures which might influence current and future operations.

Admissibility of illegally obtained evidence: the drafters of the Rules specifically chose not to set out a rule providing for the automatic exclusion of evidence illegally or unlawfully obtained and opted instead to leave the matter of admissibility of evidence irrespective of its provenance to be dealt with under and in accordance with Rules 89 and 95. It is clear from the review of national laws and international law, and the Rules and practice of this International Tribunal, that before this Tribunal evidence obtained illegally is not, a priori, inadmissible, but rather that the manner and surrounding circumstances in which evidence is obtained, as well as its reliability and effect on the integrity of the proceedings, will determine its admissibility. Illegally obtained evidence may, therefore, be admitted under Rule 95 since the jurisprudence of the International Tribunal has never endorsed the exclusionary rule as a matter of principle.

Exclusion of evidence under Rule 95: in applying the provisions of Rule 95, this Tribunal considers all the relevant circumstances and will only exclude evidence if the integrity of the proceedings would indeed otherwise be seriously damaged.

Admission of intercept evidence and right to a fair trial: in assessing whether intercept evidence is admissible, a Trial Chamber is required under Rule 89(D) of the Rules to use a balancing test to ensure that the right of an accused to a fair trial is not violated. The correct balance must be maintained between the fundamental rights of the accused and the essential interests of the international community in the prosecution of persons charged with serious violations of international humanitarian law.

[62] Article 69(7)(a) & (b), Rome Statute:

7. Evidence obtained by means of a violation of this Statute or internationally recognised human rights shall not be admissible if:
(a) The violation casts substantial doubt on the reliability of the evidence; or
(b) The admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings.

11 References

[1] W. G. Perry, "Information Warfare: Assuring Digital Intelligence Collection," The Joint Special Operations University (JSOU) Press, Hurlburt Field, Florida, 2009. Available: https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA514505.xhtml [Accessed 28 June 2016]

[2] Headquarters, Department of the Army, "ATP 3-90.15 Site Exploitation", [Online]. Available: https://armypubs.us.army.mil/doctrine/index.html. [Accessed 16 June 2016].

[3] Center for Army Lessons Learned (CALL), "Tactical Site Exploitation and Cache Search Operations, Tactics Techniques, and Procedures", No. 7-26, May 2007. [Online]. Available: http://nsarchive.gwu.edu/NSAEBB/NSAEBB410/docs/Tactical%20Site%20Exploitation.pdf. [Accessed 25 May 2016].

[4] E. Lorge, "Shining light on battlefield forensics," The official homepage of the United States Army, 27 May 2010. [Online]. Available: https://www.army.mil/article/39956/. [Accessed 17 June 2016].

[5] A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems", in IEEE Transactions on Parallel and Distributed Systems, vol. 14, no. 9, pp. 885-896, Sept. 2003. Doi: 10.1109/TPDS.2003.1233711

[6] A. Di Mauro, A. Mei, and S. Jajodia, "Secure File Allocation and Caching in Large-scale Distributed Systems", SECRYPT 2012: pp. 182-191, 2012.

[7] R. Di Pietro, L. V. Mancini, and A. Mei, "Towards threat-adaptive dynamic fragment replication in large scale distributed systems". IEEE IPDPS, 2007.

[8] T. Väisänen, "Security of a VoIP call in hybrid mobile ad hoc networks", Master's thesis, University of Oulu, Oulu, 2006.

[9] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets", In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03)*, ACM, New York, NY, USA, 2003, pp. 27-34. doi:10.1145/863955.863960

[10] L. Pelusi, A. Passarella and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," IEEE Communications Magazine, vol. 44, no. 11, pp. 134-141, 2006.

[11] V. N. G. J. Soares and J. J. P. C. Rodrigues, "Cooperation in DTN-Based Network Architectures", in *Cooperative Networking,* 2011, pp. 101-115.

[12] A. Mei and J. Stefa, "Routing in Outer Space: Fair Traffic Load in Multihop Wireless Networks," in *IEEE Transactions on Computers*, vol. 58, no. 6, pp. 839-850, June 2009. doi: 10.1109/TC.2009.17

[13] P. Zdzichowski, M. Sadlon, T. U. Väisänen, A. Botas Munoz, and K. Filipczak, "Anti-forensics study", NATO CCD COE, Tallinn, 2015. [Online]. Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/AF_with%20intro.pdf [Accessed 21 February 2016].

[14] Á Botas, R. J. Rodríguez, T. Väisänen and P. Zdzichowski, "Counterfeiting and Defending the Digital Forensic Process," *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on*, Liverpool, 2015, pp. 1966-1971. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.291

[15] E. Imsand and J. A. Hamilton, Jr., “Digital Battlefield Forensics”, *In Proceeding of the 15th Colloquium for Information Systems Security Education*, Fairborn, Ohio, June 13-15, 2011.

[16] M. Perklin, “Anti-forensics and anti-anti-forensics”, Defcon 20, 2012, [Online]. Available: https://www.defcon.org/images/defcon-20/dc-20-presentations/Perklin/DEFCON-20-Perklin-AntiForensics.pdf. [Accessed 27 April 2016].

[17] C. Zoubek, S. Seufert, and A. Dewald, “Generic RAID reassembly using block-level entropy”, Digital Investigation 16 (2016), S44-S54, *Proceedings of the Third Annual DFRWS Europe*

[18] G. C. Kessler, “Anti-Forensics and the Digital Investigator”, *Australian Digital Forensics Conference, 2007.*

[19] J. Wakefield, “Devices being remotely wiped in police custody”, 09 October 2014, BBC News, [Online]. Available: http://www.bbc.com/news/technology-29464889. [Accessed 21 February 2016].

[20] G. Zanin, A. Mei and L. V. Mancini, "A Secure and Efficient Large Scale Distributed System for Data Sharing," 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06), Lisboa, Portugal, 2006, pp. 27-27. doi: 10.1109/ICDCS.2006.11

[21] L. Cleghorn, “Example of Manipulating a Graceful Shutdown To Prevent Evidence Recovery”, *eForensics Magazine* 3(5), 2015. ISSN 2300-6986

[22] S. Azadegan, W. Yu, H. Liu, M. Sistani and S. Acharya, "Novel Anti-forensics Approaches for Smart Phones," *System Science (HICSS), 2012 45th Hawaii International Conference on*, Maui, HI, 2012, pp. 5424-5431. doi: 10.1109/HICSS.2012.452

[23] P. Knüfer, “Mitigating Anti-Forensics: A Schema-based Approach”, Ruhr-Universität Bochum, Bochum, Bachelor’s Thesis, 2015.

[24] T. Väisänen, A. Farar, N. Pissanidis, C. Braccini, B. Blumbergs, and E. Diez, “Defending mobile devices for high level officials and decision-makers”, NATO CCD COE, Tallinn, 2015. [Online]. Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/Defending%20mobile%20devices%20for%20high%20level%20officials%20and%20decision-makers.pdf. [Accessed 21 February 2016].

[25] R. Liscouski and W. McGann, “The Evolving Challenges for Explosive Detection in the Aviation Sector and Beyond”, 19 May 2016, [Online]. Available: https://www.ctc.usma.edu/posts/the-evolving-challenges-for-explosive-detection-in-the-aviation-sector-and-beyond. [Accessed 22 May 2016].

[26] A. Verma, “USB Killer Version 2.0 Burns and Destroys Your Computer”, 13 October 2015, fossBytes, [Online]. Available: http://fossbytes.com/usb-killer-version-2-0-is-here-to-burn-and-destroy-your-computer/. [Accessed 12 April 2016].

[27] Massachusetts Digital Evidence Consortium, “Digital evidence guide for first responders”, May 2015. [Online]. Available: http://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf [Accessed 17 June 2016].

[28] D. L. Watson and A. Jones, *“Digital forensics processing and procedures”,* Elsevier 2013, pp. 313 – 348.

[29] M. Smith, “PC ports explained: Get to know the back of your computer”, 06 October 2012, [Online]. Available: http://www.digitaltrends.com/buying-guides/pc-ports-explained-get-to-know-the-back-of-your-computer-2/. [Accessed 24 May 2016].

[30] O. Afonin and Y. Gubanov, “Catching the ghost: how to discover ephemeral evidence with Live RAM analysis”, Belkasoft Research, 25 June 2013, [Online]. Available: https://belkasoft.com/live-ram-forensics. [Accessed 24 May 2016].

[31] M. B. Mukasey, J. L. Sedgwick, D. W. Hagy, “*Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition’,* April 2008, [Online]. Available: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. [Accessed 02 May 2016].

[32] Forensics & Cyber Security Tools, “CaptureGUARD Gateway”, [Online]. Available: https://www.windowsscope.com/index.php?option=com_content&view=article&id=106&Itemid=90 [Accessed 24 May 2016].

[33] F. Witherden, “Memory Forensics over the IEEE 1394 Interface”, 07 September 2010, [Online]. Available: https://freddie.witherden.org/pages/ieee-1394-forensics.pdf. [Accessed 24 May 2016].

[34] F. Witherden, “libforensic1394”, [Online]. Available: https://github.com/FreddieWitherden/libforensic1394. [Accessed 24 May 2016].

[35] S. Magoun, “Ubuntu Bug #1280300 Desktop contents displayed on resume, before lock screen is shown”, 14 February 2014, gnome-screensaver package, bugs.launchpad.net, [Online]. Available: https://bugs.launchpad.net/ubuntu/+source/gnome-screensaver/+bug/1280300. [Accessed 28 April 2016].

[36] WikiHow Community Q&A, “How to remove a hard drive”, [Online]. Available: http://www.wikihow.com/Remove-a-Hard-Drive. [Accessed 02 May 2016].

[37] C. Hoffman, “It’s Time: Why You Need to Upgrade to an SSD Right Now”, HowToGeek, 18 August 2014, [Online]. Available: http://www.howtogeek.com/194750/its-time-why-you-need-to-upgrade-to-an-ssd-right-now/. [Accessed 17 June 2016].

[38] M. Byrd, “Proper Tagging and Labeling of Evidence for Later Identification”, [Online]. Available: http://www.crime-scene-investigator.net/tagging.html. [Accessed 11 May 2016].

[39] CastleView Forensics Ltd, “Investigating a Crime Scene – 7 – Packaging and Labelling the Evidence”, [Online]. Available: http://www.castleviewuk.com/ch1-packaging.html . [Accessed 17 June 2016].

[40] SanDisk Solid State Drive Quick-Start Installation Guide, [Online]. Available: http://downloads.sandisk.com/downloads/um/ssd-install-guide.pdf. [Accessed 24 May 2016].

[41] Google, “Project Loon homepage”, [Online]. Available: https://www.google.com/loon/. [Accessed 28 April 2016].

[42] Federal Communications Commission, Application for Special Temporary Authority, [Online]. Available: https://apps.fcc.gov/oetcf/els/reports/STA_Print.cfm?mode=current&application_seq=56370&RequestTimeout=1000. [Accessed 28 April 2016].

[43] Oceus Networks, “Oceus Networks homepage”, [Online]. Available: http://www.oceusnetworks.com. [Accessed 28 April 2016].

[44] Space Data, “SpySat homepage”, [Online]. Available: http://www.spacedata.net/starfighter.html. [Accessed 28 April 2016].

[45] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, “Drone small cells in the clouds: Design, deployment and performance analysis.”, arXiv preprint, 2015. arXiv:1509.01655

[46] J. M. Kahn, R. H. Katz, and K. SJ Pister. “Next century challenges: mobile networking for ‘Smart Dust’”, In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, ACM,* pp. 271-278, 1999.

[47] N. C.l Moore, “Millimeter-scale, energy-harvesting sensor system developed”, 08 February 2010, Michigan News, University of Michigan, [Online]. Available: http://ns.umich.edu/new/releases/7520. [Accessed 26 April 2016].

[48] D. Rowinski, “Connected Air: Smart Dust Is the Future of the Quantified World”, Readwrite, 14 November 2013, [Online]. Available: http://readwrite.com/2013/11/14/what-is-smartdust-what-is-smartdust-used-for/. [Accessed 26 April 2016].

[49] N. Zhu, F. Mieyeville, D. Navarro, and I. O’Connor, “High data rate wireless sensor networks research”, *Proceedings of 14ème Journées Nationales du Réseau Doctoral de Micro et Nanoélectronique* (JNRDM 2011), Paris, pp. 23-25, 2011.

[50] United Nations, “*International Legal Protection of Human Rights in Armed Conflict”,* United Nations Publications, 2011.

[51] G. Rona, “A Response to Ohlin about IHL and IHRL”, 17 January 2012, [Online]. Available: http://opiniojuris.org/2012/01/17/a-response-to-ohlin-about-ihl-and-ihrl/. [Accessed 04 May 2016].

[52] NATO MC 362/1

[53] A. Cole, P. Drew, R. McLaughlin, and D. Mandsager, *“San Remo Rules of Engagement Handbook”,* International Institute for Humanitarian Law, San Remo, 2009. [Online]. Available: http://www.iihl.org/wp-content/uploads/2015/12/ROE-HANDBOOK-ENGLISH.pdf. [Accessed 17 June 2016].

[54] International Criminal Court, “Rules of Procedure and Evidence”, ICC, 2013.

[55] Council of Europe, “Electronic Evidence Guide, Version 2.0”, COE, Data Protection and Cybercrime Division, Directorate General of Human Rights and Rule of Law, 2014.

[56] C. S. D. Brown, “Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice”, *International-Journal-of-Cyber-Criminology,* Volume 9, issue 1, 2015.

[57] E. Casey, “*Digital Evidence and Computer Crime”,* 3rd Edition, Academic Press, 2011.

[58] ICTY: The Prosecutor v. Radoslav Brdjanin - Case No. IT-99-36-T “Decision on the Defence 'Objection to Intercept Evidence'” 3 October 2003, Trial Chamber II (Judges Agius [Presiding], Janu and Taya)

12 Biographies

Christian Braccini: Christian Braccini is a Lieutenant Colonel of the Italian Army (Signals). He holds a Computer Science Degree and a Master's in Strategic Science. He has mostly served in combat units, performing several tours of duty. As a researcher at NATO CCD COE, he was involved in establishing the Centre's digital forensics capability. He has further integrated digital forensics and intelligence in numerous cyber crisis scenarios to support NATO major cyber-defence exercises.

Dr. Hayretdin Bahşi: Dr. Hayretdin Bahşi is a senior researcher at the Centre for Digital Forensics and Cyber Security of Tallinn University of Technology. He received his PhD from Sabancı University (Turkey) in 2010. He has been involved in many R&D and consultancy projects about cyber security as a researcher, consultant, trainer, project manager and program coordinator at Informatics and Information Security Research Centre of Scientific and Technological Research Council of Turkey between 2000 and 2014. His research interests include critical information infrastructure security, cyber situational awareness systems and strategic level decision-making in cyber security.

Agostino Panico: Agostino Panico is a PhD student at the Computer Science Department of University of Rome, La Sapienza. He earned his Master's Degree in Information Technology at the POLITECNICO of Turin. Before joining La Sapienza as a PhD student he took a Master's degree at the same University in 'Governance and Audit of Information Systems' (2013-2014). He is also an Officer (Lt.) of the Italian Army Technical Corps and a SANS Mentor for the 'Penetration Testing and Ethical Hacking' and the 'Hacker Tools, Techniques, Exploits and Incident Handling' courses. Panico's research activity focuses on penetration testing and incident handling on critical infrastructure.

Michal Sadloň: Michal Sadloň is working as a researcher for NATO CCD COE in Tallinn, Estonia. He has more than 14 years of experience in information security. Since 2013 he has been focusing on digital forensics research and development. He prepares and conducts courses and workshops in this area.

Teemu Väisänen: Teemu Väisänen is working as a Researcher for NATO CCD COE in Tallinn, Estonia, and studying at the University of Oulu, Finland, to graduate as Doctor of Science in Technology. He has more than 11 years of experience of information security research and development. He has been working as a Researcher for the Finnish Defence Forces and for VTT Technical Research Centre of Finland (VTT). In this study, he mainly concentrated on anti-forensics, and provided content for parts handling networking.

Mario Huis in 't veld: Mario Huis in 't veld has been employed since 1978 by the Royal Netherlands Marechaussee, deployed since March 2014 to the NATO Military Police Centre of Excellence (NATO MP COE) in Bydgoszcz Poland. He has more than 37 years of experience in various national and international positions and functions. For the last 15 years he has been working as a team member and/or team leader for crime investigations; co-worker of the National Public Prosecutor for North Sea Affairs; Liaison Officer for the Netherlands Coast Guard; Seconded National Expert to the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) and served in 2013 as a Liaison EUPOL/NTM-A/Afghan Uniformed Police in Kunduz, Afghanistan for the NLD Police Training Mission and policy advisor for the Royal Netherlands Marechaussee Headquarters.

Kris van der Meij: Lieutenant Colonel Kris van der Meij is a researcher in the Law and Policy Branch of the NATO CCD COE. He started his military career in the Dutch army as a conscript in 1985. He has served as an Engineer, in the Artillery, the Intelligence Service and as a Signal Officer before he was assigned as a Legal Advisor. He served mostly in operational units and was deployed several times to Afghanistan and Mali. He studied Military Law at the University of Amsterdam.

13 Acknowledgements

Authors of the study want to express huge gratitude to Patrycjusz Zdzichowski who provided important feedback for anti-forensics and exfiltration solutions. Professor Steven W. Wood, Utica College, and Clinton K. Watson, US Army, gave us precious guidance.