MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Hardware Forensics-an Introduction to Digital Forensics in the Embedded Computing Context

Franco DP[1]* and Dutra LM[2]

[1]Researcher and Consultant in Forensic Computing and Information Security, aCCESS Security Lab and Bank of Amazon, Brazil

[2]Researcher and Consultant in Systems Analysis and Development and Information Security-Biguaçu, Brazil

Research Article

Volume 8 Issue 4

Received Date: November 07, 2023

Published Date: December 27, 2023

DOI: 10.23880/ijfsc-16000345

***Corresponding author:** Researcher and Consultant in Forensic Computing and Information Security, Access Security Lab and Bank of Amazon-Belém, PA, Brazil, Email: deivison.pfranco@gmail.com

Abstract

The growing presence of embedded systems in the daily lives of people and companies, driven by the emergence of portable devices, makes these systems ubiquitous and a valuable source of information for criminal investigations. However, the lack of resources dedicated to forensics in this context, excluding IoT devices due to their technical particularities, led to the need to start writing this material. This article seeks to introduce experts to embedded systems forensics, highlighting the importance and existence of this field, and emphasizing that microcontrollers, flash memories, ROM memories and other often overlooked devices can contain crucial evidence for solving a variety of crimes. Furthermore, it will be discussed how to adapt conventional forensic techniques to the peculiarities of embedded systems, which generally have limited processing resources, energy constraints and high connectivity, challenging traditional forensic approaches.

Keywords: Computer Forensics; Digital Forensics; Embedded Computing; Hardware; Embedded Systems; Hardware Forensics

Abbreviations: ICT: Information and Communication Technologies; ROM: Read-Only Memory.

Introduction

Hardware Forensics is directly linked to embedded systems, which are increasingly common in the daily lives of people and companies. Thus, with the advent of the Internet of Things and portable devices, the trend is for embedded systems to become ubiquitous [1].

In this scenario, due to the popularization and high availability of devices on the market, these devices constitute a rich source of information for elucidating crimes, bringing traces that can permeate the most diverse areas of Forensic Computing - be they vehicles, aircraft, medical equipment, household appliances, wearable accessories, ingestible nanotechnology devices, etc [2].

Parallel to this ubiquity and the benefits that the technology brings, there is concern about carrying out expertise on these types of devices, since the majority of existing proposals do not take into account their peculiarities and, consequently, are not suitable for them, as differently of traditional computers, embedded systems tend to have less processing capacity and memory; restricted energy source;

and higher network degree [3].

In view of the above, this article aims to provide an overview of Hardware Forensics and forensic examinations of embedded computers (embedded systems) - a very broad category of digital systems, that is, a broad and open class of systems that is of great importance, due to its diversity and constant evolution, it is not very easy to systematize specialized methods and procedures. Systems that, in fact, are often not exclusively digital and sometimes not exclusively electronic [4].

Embedded Computing

Embedded computing deals with digital electronic systems that are incorporated into the most varied products with the aim of providing them with programmability, automation, control, or information processing characteristics necessary for them to perform their function. We are talking about the various types of systems called embedded systems, which present a wide variety of forms and functions widely distributed in all environments, and which present an extremely varied degree of technical quality - particularly in terms of the operational security they offer and ultimately, often go unnoticed by the observer who is unaware of them [5].

The state of an embedded system is easily changed by events in the environment with which it interacts. For example, opening or closing a vehicle's doors or turning on the starter can erase important event records from the vehicle's recent history. The system's dependence on its environment also makes it difficult or even difficult to skillfully examine the system when it is outside its operating environment [6].

Embedded systems, in general, are built with only essential features to fulfill their mission and serve a very specific purpose. Therefore, the means of accessing internal data may be very limited given the variety of embedded systems and, considering all these considerations, it follows that the specialized approach to embedded systems must be distinct [7].

In this scenario, embedded computing emerges to study the types of systems discussed here with embedded computers found in various electronic equipment, such as washing machines, televisions, cell phones, automobiles, and others [8].

Embedded Systems

The term Embedded System originated in the late 1960s. At that time, what existed was a small functional control program for the telephone. So, this little assembler program was being used on other devices in a customized way. Only the input and output signals defined in the program were adapted, but without modifying any line of program code. Later, with the advent of specialized microprocessors, it was possible to develop specific software in machine language for different types of processors. In the 1970s, specific code libraries for embedded systems began to emerge [9].

Current embedded systems can be programmed in high-level languages, have operating systems and are present in all human activities and, with current low technological costs, tend to increase their presence. Examples of such systems are cell phones with camera and organizer, computer systems for cars and buses, laptops, tablets, smart microwave ovens with climate control, washing machines, etc. Figure 1 shows examples of using embedded systems [10].

Figure 1: Examples of Embedded Systems.

Thus, and with continuous technological evolution, the need to design new systems in increasingly narrower time windows arose. New products have an increasingly shorter useful life, so the financial return on your project must also be achieved in a few months. For example, a technology developed for a car's ABS System (Braking and Anti-lock System) is expected to become obsolete within a few years, requiring the reformulation of a new system to be designed and applied to new car models [11].

In modern circuit miniaturization techniques, the tendency is for component terminals not to be exposed.

Figure 2 below illustrates a common case represented by a flash memory. On the left side of the figure are the memory integrated circuit terminals that are soldered to the circuit board that supports and connects various system components. On the right side is the opposite side of the memory. Once the memory is soldered to the circuit board, it is not possible to access its terminals.

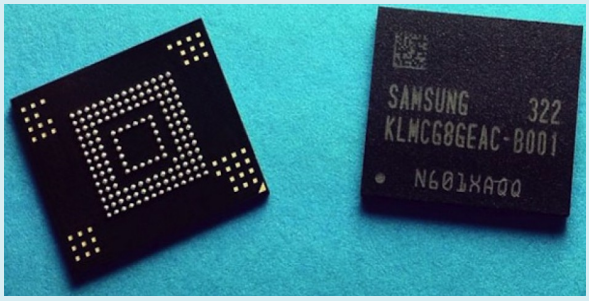

Figure 2: Flash Memory Integrated Circuit.

Taking the memory example from Figure 2 above again, its removal from the circuit board must be done using special techniques to solder all terminals without destroying the data recorded in the memory.

After this, all fuse contacts must be reconstituted using specific equipment and procedures for this function. Then, it must be placed on a specific device to read the data recorded on it. Finally, having the contents of memory available is not enough. To interpret the content, it is still necessary to know how the data is structured and coded [12].

It is important to remember that it is not always possible or feasible to read the data contained in an integrated circuit. Mainly those that incorporate a microcomputer. Classic examples are microcontrollers and smart cards. These devices typically contain mechanisms to prevent such access.

There are several commercially available microcontrollers that are very cheap, extremely compact, and very powerful. They are within anyone's reach. A microcontroller consists of a CPU, it can be programmed and reprogrammed freely and easily for any purpose. It also has a diagnostic engine that allows checking its internal data (JTAG). However, a safety device allows total and permanent blocking of reprogramming and diagnostics. Therefore, it is simple to improvise embedded, miniaturized, cheap and difficult to analyze systems. Figure 3 below shows some microcontrollers – powerful, compact and, for many purposes, complete digital systems.

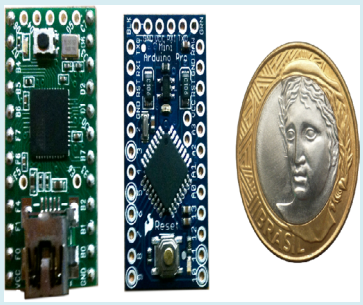

Figure 3: Microcontrollers.

Categorization of Embedded Systems

A device is classified as an embedded device when it is dedicated to a single task and continuously interacts with the environment through sensors and actuators. Because this type of system requires continuous interaction with the environment, it demands, from the designer, the structuring efficiency of the project and the code produced. The term "embedded systems" comes from the fact that these systems are designed to be independent of a power source.

The main classification characteristics of this type of system are its computational capacity and its independence of operation. Other relevant aspects depend on the types of systems, operating modes and items desired in embedded applications. Every embedded system consists of a processing unit which is an integrated circuit connected to a printed circuit board. They have software information processing capability processed internally in this unit; hence the software is embedded in the processing unit. All embedded software is classified as firmware.

Integrated and embedded and embedded systems are subdivisions of the dedicated systems category.

They are all systems built with the purpose of fulfilling a specific task. What distinguishes them is the degree of dependence of their architecture and physical implementation on the environment in which it operates and the task it performs. These concepts have some similarity to each other, but the distinctions are very relevant due to their implications for specialized technique. Thus, here we make a clear distinction between the concepts of embedded system and embedded system, but it is important to highlight that the technical literature is sometimes not very rigorous in the use of the terms. Although this distinction is very important in the field of specialization, it is of little relevance to most engineering of these systems.

Integrated Systems

An integrated system is nothing more than a system composed of a standard software and hardware base that has been adapted to perform a specific task. A common example are ATMs in supermarkets and small businesses, which essentially consist of a computer that runs a program that operates under the control of an operating system, normally equipped with application-specific peripherals, and connected in a conventional way through standard interfaces.

Embedded systems are very similar to ordinary computing systems, differing little in terms of architecture, components, connections, and operating principles.

Therefore, the examination of this type of system can and should be carried out using the expert techniques usually used in the examination of computer systems. These specialized techniques are covered extensively in other chapters of this book, so we will not stop here with this category of systems.

Embedded Systems

Embedded systems generally do not communicate with the outside world through the usual means employed by personal computers. Instead, they interact with the environment through integrated sensors and actuators and interfaces that employ specialized communication paths and protocols. Furthermore, embedded systems are built with resources reduced to what is strictly necessary to perform their function, which is why they often have very little internal memory, and their processing capacity is very limited compared to common computers.

Embedded systems differ from integrated systems because they are physically incorporated into the equipment in which they are housed and designed from the beginning to perform specific tasks. They are not, therefore, mere adaptations of general-purpose systems. A typical example of an integrated system is the control system embedded in the mechanical arm of an industrial robot. Another common example is the electronics built into modern microwave ovens. To give a more sophisticated example, we can mention the internal system of so-called Smart TVs.

Although embedded systems are present in a multitude of everyday devices, most people are unaware of these systems, much less recognize them as computers. However, an embedded processor is nothing more than a computing device embedded as part of a system that it controls, carrying out logical operations established in accordance with a fixed or changeable program, acting and reacting in accordance with the logic and variables of the controlled process.

Real-Time Embedded Systems

An embedded system is real-time when it is designed to ensure that it responds to requests and changes in its environment within well-specified time frames. In other words, the system is fast enough to meet your application needs and never fails to respond.

Real-time systems can be classified as “soft” and “hard”. Soft real-time systems are those that respond at times suitable for human interaction but are not too rigid. There is some flexibility in the response time, which can be greater or lesser within a range, and can even be variable between successive operations, without impacting the usefulness or security of the system.

Hard real-time systems are those in which there are strict control objectives that must be achieved within specified and deterministic deadlines, under penalty of deterioration in performance or risk to equipment, other assets or, mainly, the physical integrity of people. For example, the reaction and actuation times of an assisted braking system in modern motor vehicles are fractions of a second and must be adhered to. Therefore, this system must be real-time and “hard”.

Embedded Systems Themselves

Embedded systems themselves are a subcategory of embedded systems, that is, embedded systems are the genus, embedded systems are a kind of genus. Embedded systems are, for example, systems embedded in vehicles.

Talking about embedded electronics means dealing with electronics that are on board hardware, that is, when it comes to embedded electronics, we are talking about electronics incorporated into the hardware itself, and not just on board. When we talk about embedded systems, we are talking about embedded systems that make up the functionality of the hardware.

It cannot be said, for example, that the desktop computer used to manage customer accounts at a cruise ship bar is an embedded system. This is an ordinary computer with some application software running under the control of a standard operating system. At most, we could say that it is a system integrated into the ship’s general passenger account control system. Forensics analysis of this hypothetical ship’s bar computer can and should be done by treating it as an ordinary computer, not as an on-board electronic item.

Hardware Forensic Analysis (or Embedded Forensic Analysis)

The definitions presented above are only attempts to define the concept of embedded systems. An exact definition is impossible given the many manifestations and rapid technological developments. For forensic examination purposes, it is practical to distinguish between open and embedded computer systems based on the presence of interchangeable components for data input, output, and storage.

According to this definition, an embedded system is a computer system without these interchangeable components (keyboard, screen, hard drive, etc.). The introduction of PDAs (Psion, Palm, Pocket PC, etc.) is an example. Before these PDAs appeared on the market, there were almost no interchangeable components for electronic diaries. It was then almost impossible to use forensic tools “from the world of open systems” to investigate these embedded computer

systems. Since the introduction of interchangeable memory cards, this has become possible, and it can be assumed that electronic diaries are evolving from embedded computer systems to open computer systems.

The emergence of the Internet provided embedded systems developers with the ability to provide a web interface over a network connection. This avoids the cost of a fancy screen yet provides a complex and complete interface to be accessed on another computer. Table 1 shows network usage by type of embedded system.

IoT	With Network Not Being IoT	With No Network
Smart Thermostats	Network Routers and Switches	Microcontrollers in Home Appliances
IP Security Cameras	Industrial Control Systems	Automotive Controllers
Smartwatches and Smart Clothing	Smart TVs	Remote Control of Devices
Connected Health Meters	Connected Medical Devices	Digital Thermometers
Agricultural Sensors	Network Game Console	Elevator Controller

Table 1: Network Usage.

The types of systems covered in this article generally reside on machines that can run continuously for years without errors and can sometimes recover on their own after errors. Therefore, software is generally developed and tested more carefully than on personal computers. Error recovery can be achieved with techniques such as the watchdog timer, which restarts the system unless the software periodically notifies an identifier.

In view of the above, the expertise in this type of environment is already technically more complex than the expertise in personal computers, for example. What makes the distinction between embedded systems and embedded systems relevant from a specialist's technical point of view is that the installation and operating conditions of embedded systems bring even greater challenges and difficulties to specialized work.

Professional Specialization

The forensics analysis of embedded systems requires extensive knowledge of electronics, digital systems, automation, and control. Requires mastery of specific investigation skills applying the scientific method. It also requires permanent professional updating.

The forensics analysis of computerized systems, when its purpose does not require the examination of the hardware itself, often does not require advanced knowledge of electronics. In contrast, the inspection of embedded systems can only be carried out by electronics engineer with specific knowledge in this type of systems. In fact, the circumstances of the case and the partial results of the examination may even point to the need for an in-depth examination of the system components, a situation that only a specialized professional can determine, in which case even knowledge of microelectronics and access to specialized laboratory resources for internal analysis of integrated circuits [13].

There are no ready-made recipes. There are no universally accepted software tools. It is necessary to have the technical capacity to be able to treat each expert case as unique, guaranteeing the quality of the result in a position to withstand possible challenges.

Table 2 below, summarizes the degree of technical complexity of the forensics analysis of the different classes of system, indicating the degree of professional specialization necessary to fulfill this task. Table 3 below, classifies the complexity of the embedded system.

System Class	Technical Complexity	Expert Specialization
Common	Smaller	Information Systems
Integrated	Median	Information Systems
Embed	Bigger	Electronic Engineering
Embarked	Much bigger	Electronic Engineering

Table 2: Technical Complexity of the Forensics Analysis of the Different Classes of System.

Simple	Mean	High
Washing machines, microwaves, and toasters	Portable Medical Devices	Smartphones
Universal Remote Controls	Smart Thermostats	Car Entertainment Systems
Digital Watches	RFID/Biometrics Access Control Systems	Advanced Medical Devices
Simple Electronic Toys	Printer Drivers	Aircraft avionics systems
Motion Sensors in Luminaires	Programmable Thermostats	Industrial robots

Table 3: System Complexity.

Specificities

The computer forensic techniques used to examine common computer systems are well developed and have many tools for preserving, extracting, and analyzing data of specialized interest. Standard procedures and best practices were developed to ensure the fidelity and usefulness of initial exam results, the same does not happen for the embedded systems category, and even more so for the embedded systems subcategory.

In general, the expertise of traditional digital systems is in systems that are inactive at the time of analysis. Expert analysis is usually not done directly on the system, but rather on a static image that reflects the state of the system at a given point in time. Therefore, one of the first steps recommended by our forensic best practices is to produce a true picture of the state of the system at a given point in time.

Another fact observed over the years in forensics of traditional systems is the constant increase in the amount of information that must be processed during forensics. The result is two notable features of recent computing skills: firstly, the need to process ever-increasing amounts of data and, secondly, the increasing prevalence of standardized and automated procedures for data extraction and analysis.

The first and most crucial difference, in the case of embedded systems, and especially embedded systems, is that, due to the connection of the system state to the conditions present in the environment it controls, it is often necessary for the system analysis to be carried out with it active and connected to its normal operating environment. Therefore, preserving the state of the system at any time, as required by the usual good practices in computer science, simply cannot be applied. Additionally, there is a risk that the specialized procedure will dangerously interfere with the operation of the system [14].

A notable exception occurs in cases of motor vehicle collisions. To overcome these difficulties, during normal operation, vehicles continuously record some important information in volatile memory (RAM), such as instantaneous acceleration, speed, vehicle attitude, etc., keeping the data corresponding to the last five seconds of vehicle operation organized chronologically. In the moment of the collision, this data is transferred to permanent memory (PROM, EPROM or EEPROM) and remains permanent for later examination. This function is normally performed by the unit responsible for controlling the airbag activation.

The second difference observed in embedded systems is that there is no standardization of access paths to system state variables, or at least they are not standardized as widely as the access routes used in common systems. Finally, the physical and functional structure of embedded systems is very diverse, varying with the type of equipment, model, version, or manufacturer. Typically, the amount of data that must be captured and processed during embedded systems expertise is not very large. However, recently, in automotive electronics there has been a significant increase in the complexity of the software used.

This happens mainly in embedded information and entertainment systems, where there are already control units running programs that bring together more than 2 million lines of source code.

General Approach

Given the diversity, variability, and constant evolution of embedded systems, it is not possible to establish rigid protocols for carrying out their expertise and having a general application. However, the basic principles that govern this type of examination must always be observed [1]. Based on these principles, it is possible to establish a general approach that is sufficiently flexible for the expertise of less common embedded systems.

The first thing to do when beginning a technical system exam is to determine if there are specific resources available for the type and model of equipment exam. It is important to determine which laboratory instruments, tools, software, and other supporting materials are necessary or appropriate for this examination. Often, within limitations, tools used to diagnose and repair defects can be used.

The equipment manufacturer is generally a primary and reliable source of useful information for specialized work. However, for a variety of reasons, this information is often very difficult to obtain.

Manufacturers treat the technical details of their systems as industrial secrets. Sometimes the company that puts the system on the market is not the manufacturer itself and just applies its brand to a product that is manufactured by a third party. Other times, the manufacturer is a systems integrator that uses modules provided by third parties to compose its final system, with the manufacturer not being able to provide technical information on the modules used.

As it is impossible to obtain technical information about the equipment, it is necessary to reverse engineer it. This is a very costly operation in terms of resources and time, and extremely inconvenient given the uncertainties it introduces regarding the validity of the expert results [2]. Therefore, it is important to determine which parts of the system are relevant to the examination and which components of the system can be a useful source of information.

Memory circuits, and more specifically semi-permanent flash-type memory circuits as shown in Figure 4 and read-only memory circuits, are perhaps the main objects of specialization in embedded systems. This is where information of expert interest is generally recorded. Memories of this type include, for example, contact lists and messages received on a smartphone, geolocation records of mobile equipment, access records to an area with controlled access, dynamic data from a car accident, etc.

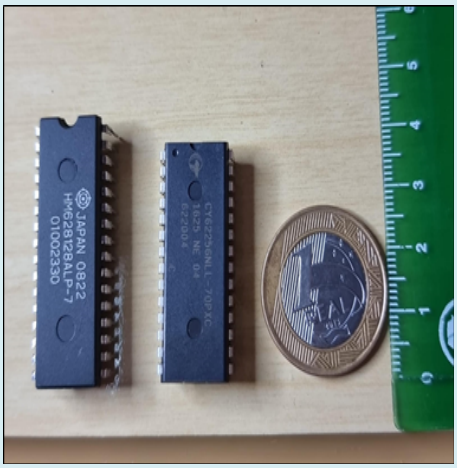

Figure 4: RAM Memories, of the Flash Type (SRAM Model in the Image) Found in Embedded Systems.

In some cases, it is possible to access the contents of these memories by making direct connections to their electrical terminals. However, two conditions are necessary for this to occur. The first condition is that the existing connections with the rest of the circuit do not generate interference in this access. The second condition is that the memory terminals are exposed so that they are accessible. It is increasingly common that the second condition is not met.

In other cases, when the memory is of the read-only type (ROM, such as EPROMs/EEPROMs, see Figure 5, it is possible to remove them by detaching them from the socket, or desoldering them, and placing them in a reader/writer. EPROMs as shown in Figure 6, the XGecu Pro TL866 commonly used to read, extract, and write information to them, which are of utmost importance in forensics.

Figure 5: Read-Only Memories (ROM).

As mentioned, there are situations in which forensics may require the removal of the equipment component so that it can be examined in isolation. The first situation is when the system does not allow access to the data of interest, due to the way it was built. The second situation is when the equipment is inoperative or partially destroyed [6].

The solution in these cases is to remove the component from the circuit board where it is installed so that it can be examined outside of the original system. Removing memory components is extremely complicated and risky. The chances of failure, including destruction of components, are very high. This operation should only be carried out as a last resort by qualified and experienced professionals and requires a sophisticated laboratory infrastructure.

Evidence Acquisition

Cyber footprints are fragile and can easily be altered, damaged, or destroyed. For this reason, perhaps the main and first recommendation in all computer manuals is that special care be taken to preserve such traces.

The first thing to do is to prevent the traces from being

altered through incorrect handling, whether accidental or on purpose. This becomes even more critical for embedded systems because they respond to changes in the environments they monitor or control, therefore their internal state is very susceptible to events in their environment.

Take, for example, the onboard electronics of a car. Simply opening a vehicle door can alter relevant data recorded in on-board systems. Likewise, the initial activation may erase records of the vehicle's previous use history. It should be noted that the effects of these events also depend on the model and year of the vehicle and can only be predicted through a meticulous study of the manufacturer's documentation. On the other hand, prior access to this documentation is quite difficult because this type of information is not publicly disclosed by automakers or component manufacturers. Essential information is treated as industrial secrets and its access is restricted even to specific sectors of these organizations.

This difficulty in access is a serious problem because it brings a series of difficulties to expertise that go beyond mere operational issues. The first and most obvious is that it hinders the development and, mainly, the validation of the procedures and tools used in forensics. The second difficulty is that it induces the expert's dependence on the cooperation of manufacturers, which tends to undermine the expert's independence, often causing deviations from the authorship of the exam, even making it impossible to carry out the test independently.

As we said previously, and it is worth repeating, the expertise of embedded systems is quite different from that of integrated systems, and even more so than that of common computing systems. Embedded systems have specific architectures, very restricted means of access and much more limited resources. Add to this the fact that embedded systems operate in close relationship with their environment, which makes it very difficult to reproduce the system's operating conditions in a laboratory environment.

Therefore, embedded systems expertise is also much more complex than common computer systems expertise because it also requires, in addition to common knowledge of computer systems, a solid and more comprehensive knowledge of electronic systems. In this way, embedded electronics goes even further, and its forensics analysis presents additional challenges to those presented by expertise in embedded systems.

When a failure occurs in a mechanical system, the failure is usually caused by some change in the material that is readily apparent and traceable. As the system continues to operate, there is often clear degradation of the system, further highlighting the failure rather than masking the failure by some phenomenon leading to self-repair or trace concealment.

In electronic systems, failures can be intermittent, that is, they occur when certain conditions are present, but not always when they are present. This often makes it difficult to identify the fault. If they are not observed when they occur, they cannot be observed later. They often leave no trace. When they come out, they are usually not noticeable without the use of instruments. If there is a trace, the fault can only be identified if it is the only possible way to produce the trace found.

Embedded electronic systems are subject to conditions that favor intermittent problems. Vibrations, weather conditions, abuse and other factors induce intermittent failures that, in electronic systems, do not leave easily visible marks. Unless the system itself predicts the occurrence of this failure and records it appropriately for later capture in a technical examination, the occurrence of the event cannot be proven with reasonable certainty.

Recovery of Information Contained in Roms

Using the XGecu Pro TL866 reader and writer shown in Figure 6 it is possible to retrieve information from a series of types of ROMs (EPROMs/EEPROMs), inserting them into the reader, connecting them to the computer with its USB cable, turning on -as and recovering the memory dump using the Xgpro software (also known as, XGecu Universal Programmer, shown in Figure 7).

Figure 6: XGecu Pro TL866 Reader and Writer.

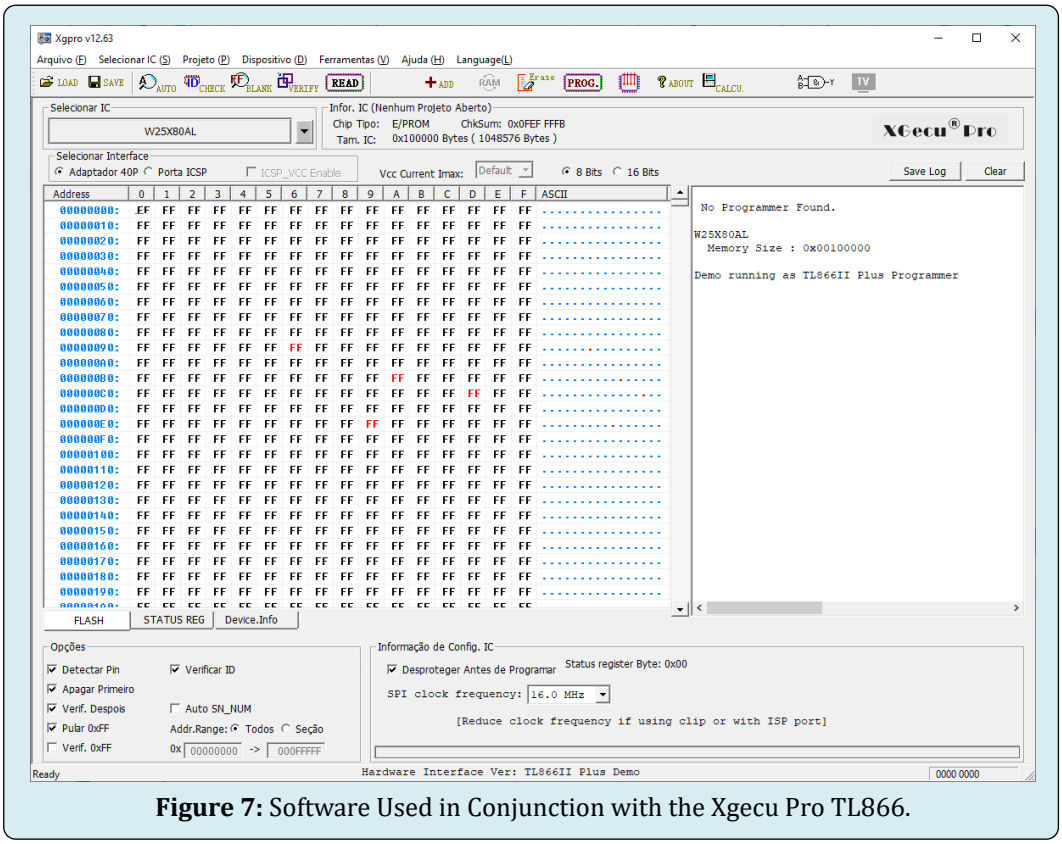

Figure 7: Software Used in Conjunction with the Xgecu Pro TL866.

Such memories, as mentioned previously, can contain valuable information for forensics, as they reveal information about the devices to which they are interconnected.

Information Reconstruction

Due to the extremely rapid development of Information and Communication Technologies (ICT), new products that may contain cyber traces arrive on the market every day. It is impractical to analyze all these products according to their forensic possibilities. Furthermore, it is rarely acceptable to spend a significant amount of time at the beginning of a forensic investigation researching specific embedded systems to determine what data can be extracted from them. The use of these criteria seems feasible to find a middle ground for the goal-oriented selection of the methods and techniques to be developed.

It is not always possible to determine in advance which traces are relevant. The traces linked to an individual are often more important than the traces of the system. An 8-byte phone number will generally be more interesting than a four-megabyte MP3 audio file, but this may not apply to a four-megabyte TIFF file from a digital camera. The possibility of recovering deleted files is also important. In the 1990s, electronic organizers were very popular and often provided researchers with useful information, especially from address files.

It is much more effective to develop methods and techniques for components that occur in as many products as possible and that also satisfy the first criterion than to develop methods and techniques at the product level. For embedded systems, memories are the first candidates among the components and mainly rewritable non-volatile memories. At a much higher level, the operating systems that occur in various products are important for the development of methods and techniques.

For the design, testing and production of embedded systems, methods and techniques are used that are also useful in the development of forensic investigation methods and techniques (connectors, desoldering equipment, analyzers, simulators, debugging interfaces, etc.).

Sometimes a method can be automated to such an extent that it can be applied with a PC and perhaps some supplementary hardware by someone without advanced technical knowledge. This gives people with advanced technical knowledge more time to develop new methods and techniques. In the case of embedded systems, commercial techniques for exchanging data between embedded systems and PCs are important (e.g. for diagnostics, backup and synchronization). Both ZERT and TULP make use of these

techniques. With these commercial techniques, data is exchanged mainly at the file level, so specialized knowledge and equipment are required to recover all data.

Therefore, there are two reasons to make a distinction between data stored in an embedded system and data linked to an embedded system (proximity data):

- Data has a different meaning in legal terms. In forensic examinations, all means can be used to retrieve and display data stored in memory. However, when it comes to related data that is not stored in the evidence itself, restrictions often apply;
- The technical aids for reading the data are different. Already available equipment can often be used to read neighborhood data.

Figure 8 presents a schematic of the steps of hardware forensic investigations.

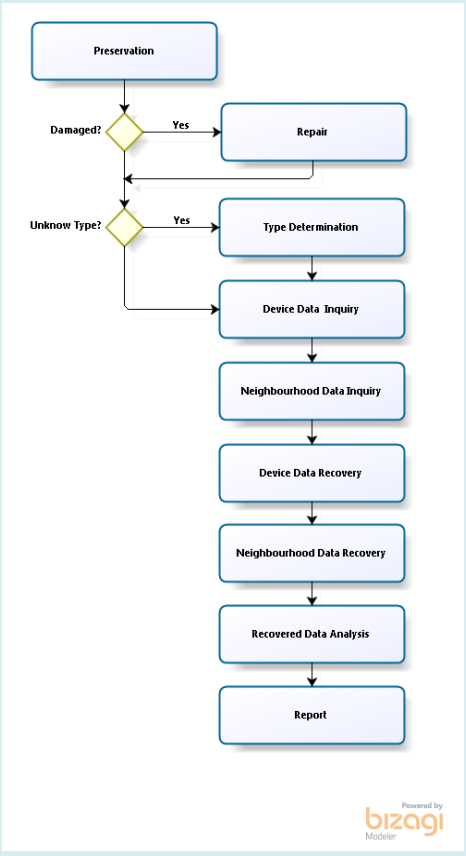

Figure 8: Steps in Hardware Forensic Investigations.

Preservation

Record all visible data (contents of displays, status of light sources (LEDs), position of switches, external damage, etc.) and attempt to verify that the system has a power source and take precautions to ensure that this power source does not fail. This will prevent the loss of any data stored in volatile memory. In addition to personal data, this data may also refer to any security system previously accessed by the user (password, PIN). If the device is turned on, the security system does not influence data extraction; once turned off, the access procedure must be redone [10].

Try to establish whether the system has I/O components that could affect the data present. In addition to system data, individual personal data can be changed. This may or may not be desirable depending on the situation. With a cell phone, for example, it may be desirable to allow this data to be stored by the phone until a request to the service provider for complete acquisition of all transaction data related to the cell phone takes effect.

An effective method of protecting cell phone data from changes over the network is to wrap it in aluminum foil. However, this can cause the battery to drain more quickly because the phone is consuming more power searching for the network. Therefore, the phone needs to be moved as quickly as possible to a protected area (in which all network and network connections are shielded) and connected to a network adapter.

Many navigation systems (cars) contain cyclic memory in which the last route traveled is permanently stored. When this data is relevant, it is important not to move the system and investigate whether it is possible to protect the cyclic memory against changes. If this is not possible, there is nothing to do but read the system in place.

Repair

With victims of violent assaults, cell phones are occasionally found that were likely damaged during the crime. Since every cyber trace may be relevant in this case, attempts are made to repair evidence if it is not possible to extract the data in any other way.

As forensic software for reading SIMs is known, during arrest the suspects try to disable your SIM (by biting it, stepping on it, etc.). Therefore, SIM cards often no longer work, but they can be repaired. First, the plastic cover is removed with a scalpel on the side of the card opposite the contact surfaces. Second, the epoxy material protecting the chip is removed using an etching solution in a chemical fume hood.

The damage can then be assessed under a microscope. If the silicon surface has been torn or pulverized, no further repair attempts will be made (although very labor-intensive methods exist to allow partial data recovery). If the only

damage is a break in the wires connecting the silicon and contact surfaces, small needles (microprobes) are placed into the chip at the points where the connecting wires used to be attached.

These probes are electronically connected to a smart card reader through which the SIM can then be accessed.

Type Determination

Most embedded systems contain sufficient visual markings to allow type determination. When there is no visual indication of make, model or type present on the system (regardless of whether it has been deliberately removed or not), digital identification techniques can be used.

Black boxes, electronic devices whose functionality is unknown at the start of the investigation, form a separate category of evidence, as do X-ray photographs – which, particularly in fraud investigations, are found to involve equipment encapsulated in opaque epoxy. X-rays can then provide useful indications and serve as a tool for further investigations (e.g. selective removal of specific pieces of epoxy). X-ray photographs can also be used to identify smart cards that do not have contacts.

Querying and Retrieving Device Data

Once evidence has been identified and found to be of a type not previously encountered, an investigation needs to be carried out into what data it may contain and how that data can be accessed and read. When it comes to a commercial device, the preferred approach is to obtain the same type of device – a specimen that can be compared with the evidence. It is often possible to determine from the technical manual what types of data may be present and how these may be protected, changed, and read by the user.

Furthermore, technical documentation from the development or maintenance and repair phase is valuable for recovering data that is not of direct importance to the normal user. Read investigation can be divided into gaining access and extracting data.

Gaining access involves penetrating the security that protects stored data. This is particularly important when using the normal input and output mechanisms of a device, such as a PIN code to access a smart card. These logical security measures are bypassed when data is read directly from memories. Alternatively, it may be necessary to bypass physical protection, for example by removing an epoxy layer from a smart card. Various methods and techniques for gaining access are:

Procedural: in several cases, access is controlled through judicial procedures. This applies, for example, to accessing a smart SIM card.

Back Doors: Many systems to secure access have a deliberately constructed back door with which security can be bypassed. In some cases there is a backup password (also known as master password) provided in the technical documentation that always works.

Measuring Memory: A password checking algorithm works roughly as follows: the correct password is stored in non-volatile memory and the password provided by a user is stored temporarily.

Memory Injection: it does not always seem possible to recover the password using the method described above; for example, when the password is not written directly into memory, but is hashed or encrypted. Password location can often be established by taking further measurements with different passwords. In these cases, the password can be replaced with data from a known password.

Correlation Measurements: The memory methods described above only work if the address bus and data bus can be accessed by the measuring equipment. In compact systems, in particular, all memory components can be integrated into the CPU on one chip and covered with a layer of epoxy (single-chip types). When dealing with these types of single chips, accurate measurement of CPU-related signals (instead of memory measurements) offers a solution. When dealing with the password checking algorithm described above, it becomes clear that a certain amount of time passes before the CPU reports that the password is incorrect. The more correct characters there are, the longer the verification process will take. By measuring the time required to verify an entered password, it is possible to check how many characters of the entered password are correct.

Brute Force: with the brute force method, a series of passwords (exhaustive or not) are entered into a system. When the order is chosen so that the most likely passwords are tried first, this is known as password guessing. The brute force method has the great advantage that it is non-destructive and can therefore be tried first on an unknown system of which there is no other known example available. Depending on the type of system, the password can be entered mechanically or electronically.

Once you have access to evidence, you need to extract as much data as possible, preferably without changing anything in the evidence. The most obvious method is to take a memory dump (also known as an image) of all evidence data. But some complications can also arise in embedded systems. Memories cannot be accessed directly because, for example, there are no technical methods available for this or because other data may be lost when accessing them. The latter applies particularly to equipment with volatile memory, for example, because volatile memory can only be read if it is

removed (causing the loss of all data); or because the device needs to be opened to access non-volatile memory, causing all data to be lost when the power supply is interrupted.

There are no methods available to reproduce information contained in memory dumps. Information from a PC disk image can be analyzed by restoring the image to another PC. By standardizing file formats, most information can be made visible in a very simple way. This standardization is less common in embedded systems.

Thus, in practice, the following methods and techniques are used to reveal data contained in embedded systems:

Using the User Interface: leave the system turned on and use the normal user interface so that no data is lost. Furthermore, the system itself provides the transformation of data into information (decoding) so that the data does not need to be processed later. Examples of equipment in which this method is applied in practice: telephones and navigation systems. The investigator needs to have the system's technical documentation and have experience in manual reading. This will prevent data from being lost or unintentionally affected. All operations must be documented, and the final report must state that the data was read manually. The manual reading method does not guarantee that all data contained in the system is recoverable, and there is the possibility of human error.

Use of Existing I/O Interfaces with Commercial Tools or Proprietary Software: commercial tools for data exchange are available for many embedded systems. For example, software for synchronizing data between mobile systems and PCs. This software works in the same way as standard media analysis. The system to be investigated is backed up and then placed on an exemplary system of the same type for later analysis. It is often possible to analyze these backups on a PC or (partially) convert them to a more common format. This usually involves file backups, as opposed to bit-for-bit "image" backups, so it is possible that not all data will be read. An increasing number of embedded systems include a chip card slot with which backups can be made to a chip card.

Direct Memory Access: This method can be applied when a memory can be physically reached and there is a method to remove the memory or connect it to external equipment. This method requires specialized equipment and skill and is therefore only used in laboratory settings.

Querying and Retrieving Data from Proximity

In addition to being a data carrier, evidence can serve as a means of accessing external systems that may contain data. Thus, a GSM phone with SIM, for example, is seen as a means of accessing the following data stored by the operator: voicemail messages, call forwarding and credit. In addition to this linked data, the following dialing details for each outgoing call are stored by the service provider: the IMSI and IMEI of the caller; the number called; the date, time and duration of the conversation, and the transmitter cells where the conversation began and ended.

Proximity data is often only kept for a limited period, so it needs to be protected as soon as possible. Due to the functioning of some of these means of access, it is possible that there are other judicial conditions for investigating this data. Some examples serve to illustrate the reading of linked data:

Voicemail Messages: Digital recordings can be made by connecting a GSM phone to a PC's sound card. The menu structure used to listen to voicemail may vary depending on your carrier.

Smart Cards: The previously mentioned SIM is a specific application of the smart card. Smart card is a tamper-proof minicomputer that is generally embedded to perform the security functions of identification, authentication, authorization, integrity, and confidentiality. A smart card is often connected to other information systems with supplementary data storage.

Analysis of Recovered Data

If a report of all data read from evidence by non-technical investigators is not sufficient for a judicial investigation, additional analysis by digital experts may be necessary. It can be difficult to find relevant information due to the large amount of (technical) data. As memory sizes continue to increase, this will also become an issue with embedded systems (just as it already is with media analytics). Additional analysis and filtering techniques will be required to allow the search to focus on obtaining information within the large amount of data. Another reason for additional analysis is the customer's lack of technical knowledge. Two examples are given below:

Call Data: When telephone conversations play a crucial role in providing evidence, it is necessary to know the meaning of all the elements that appear in print and be aware of any imperfections that such a list may contain. A technical expert will, for example, give more probative value to an IMSI than to an IMEI because he is aware of the possibilities for changing an IMEI and the extent to which this knowledge is disseminated via the Internet.

Fraud: In fraud investigations where embedded systems play a significant role, questions are raised such as 'is it possible to commit fraud Y with system X' and 'could the data from system X be related to the data found with suspect Z.' Some practical examples of X/Y include 'a small black box with a smart card reader,' 'telephone card updates,' and 'a box with remote control'/'Tampering with a mileage recorder.'.

An expert needs to stay up to always date with the

latest technical developments. For example, there is a known method to recover the SIM secret key with a specific authentication algorithm. Combined with the ease with which a SIM can be programmed nowadays, it is not impossible to clone a SIM. What a non-technical person may not realize is that printouts can also be used to retrieve related networks.

Criminal organizations appear to know GSM phones are monitored. For this reason, they use a collection of GSM phones and a collection of anonymous prepaid SIMs that are changed very frequently. GSM phones found after an arrest increasingly lack SIM. In addition to the previously described GSM phone data recovery methods, printouts can be a useful contribution here. Based on a found IMEI or IMSI, a lookup operation is mounted on the service provider's call data. If the search result includes new IMEIs or IMSIs, the search operation can be mounted with the newly found data. In this way, a network of GSM phones and SIM cards can be mapped, possibly even registered with a name.

This type of investigation often begins with collecting as much information as possible. Thus, it is necessary to reconstruct the electrical diagrams from the discovered electronic equipment (the construction of a not very complex printed circuit board can be recovered manually with a multimeter and established with the aid of software for designing electronic connections) and the reconstruction of the embedded software (it is often not possible to read embedded software directly with microcontrollers with integrated program memory because these can be read-protected).

If source code for embedded systems of the same type is discovered on other systems encountered (e.g., PCs), the following method can be used to discover whether the code in program memory is based on the source code that was discovered.

The discovered source code is translated into machine code with the same development tools found on the confiscated system. A microcontroller of the same type is programmed with this machine code.

Two measurements are then made on as many input and output pins of the microcontroller during use within the microcontroller of the embedded system under investigation. For the first measurement, the discovered microcontroller is used, for the second it is replaced by the programmed microcontroller.

The measurement data consists of lists containing all times that this pin's value changed for each pin. When the measurement data for both measurements are identical, one can conclude with probability close to certainty that the software embedded in the microcontroller being investigated is based on the source code found.

Report

In the forensic investigation of evidence, each step must be documented from the moment the evidence is delivered. The following script is adopted:

- Upon arrival, an application form is filled out which includes the following data: name and address of the applicant, client and contact person; date and means of delivery; description of the infraction; name of the suspect and/or victim; description of the evidence; the issue and the urgency.
- This data is centrally entered into a case management system. The subsequent processing of evidence is recorded in this system so that it can be determined for each treatment when it was carried out and by whom.
- An investigator is appointed at department level for (partial) investigation. In addition, a duplicate investigator, and an authorized signatory (who can also be the investigator or duplicate investigator) are appointed. Meanwhile, the evidence is provided with a unique barcode and a folder for storing all non-electronic documentation. The investigator can print record forms from the case management system in which all stages of the investigation carried out with the evidence are noted (electronically or on paper, depending on your choice). Specific registration forms may be provided depending on the type of case.
- The investigator compiles a draft report on the investigation and sends it to the investigator in duplicate along with the complete file. Integrity tags (SHA hashes) are provided for any digital appendages (writable CDs). These identification marks are indicated on the report by recordable CD.
- The duplicate investigator checks the investigation and report and discusses any changes with the investigator.
- The authorized signatory, who has undergone internal training culminating in an examination at expert level, evaluates the result and signs the expert report only when he is in full agreement with the content of the report.
- The report and evidence are sent to the client, the folder and all digital data collected during the investigation are archived. It rarely happens that an expert is questioned during legal proceedings.

Conclusion

It is virtually impossible to imagine the modern world without embedded systems. Most people simply enjoy the everyday facilities provided by these systems without even realizing it. Computing in practice goes far beyond the machines that we can effectively recognize as computers; it

has become part of modern life and shows no signs of leaving us anytime soon. Note that these systems are now becoming part of our clothes and I believe that in the not-too-distant future we will incorporate them into our own bodies, giving them never-before-seen characteristics [12-14].

Embedded systems present a huge variety of formats and functions, technical quality, access, and operation security. This combination of characteristics makes it practically impossible to establish rigorous protocols for their specialized processing. Recipes are impossible. Specialized work can only be sustained in the real mastery of scientific principles and methods, and not just in the blind following of pre-established routines.

The use of metrics and the development of test artifacts assist in the process of acquiring software quality - fundamental for the survival and success of the system, whether embedded or not, considering that its development is increasingly globalized. For an organization to stand out in this market, it must produce software that meets customer expectations regarding the quality, reliability and security of the products and services offered.

Forensic investigation in embedded systems is still in its infancy. Only a few people work in this area and almost no companies supply products in this area. Possible reasons are the limited number of experts, the huge diversity of systems and the lack of a large market. The potential for finding cyber traces in embedded systems is only known to a small group of the law enforcement community. As cyber traces from embedded systems are increasingly discussed during legal proceedings, it is anticipated that calls will be made more frequently to experts. This is further reinforced by technological developments that provide for the integration of data from embedded systems and personal computers.

The phone will be integrated into a mobile desktop with a permanent Internet connection for the user. Gradually, security functions will be added to this equipment for advanced biometric identification applications. The personal nature of such a system makes it particularly interesting for digital research. Given the huge investment involved in low-level physical investigation methods, these investigation methods will not be viable in the long term due to the miniaturization of electronics.

Since this also applies to the development and maintenance of these systems, alternatives are being developed which, in turn, can be used for forensic investigation. In the long term, embedded systems may become the most important sources of digital investigation because these traces are largely not accessible to the user and are therefore less susceptible to manipulation.

References

1. Good practice guide for computer-based electronic evidence. ACPO.
2. Eoghan C (2009) Digital forensics and investigation manual. Academic Press.
3. Lemos Coast MAS (2011) Forensic Computing - Forensic Analysis in the Context of Computer Incident Response, In: 3rd (Edn.), Millennium, São Paulo, Brzail.
4. Daniel L, Daniel L (2011) Digital Forensics for Legal Professionals - Understanding Digital Evidence from Warrant to Courtroom. Elsevier, United States, pp: 1-368.
5. Venema Wietse FD (2007) Computer Forensics - Theory and Applied Practice - How to Investigate and Clarify Occurrences in the Cyber World In: 1st (Edn.), São Paulo: Pearson Education do Brasil.
6. (2000) FBI Forensic Science Communications - Digital Evidence.
7. Bos H, Ioannidis S, Jonsson E, Kirda E, Kruegel C (2009) Future threats to future trust. Future of Trust in Computing pp: 49-50.
8. ISO (2013) ISO/IEC 27037 2012 Information Technology - Security Techniques - Guidelines for identifying, collecting, acquiring, and preserving digital evidence. In: 1st (Edn.), Sec aware policies, Brasil.
9. Solomon J, Lattimore E (2020) Computer Forensics. pp: 1-12.
10. Vlachopoulo KC, Magkos E, Chrissikopoulos V (2012) A Model for Hybrid Evidence Investigation. International Journal of Digital Crime and Forensics (IJDCF) 4(4): 16.
11. Paulo L (2011) Computer Crimes and Computer Security. São Paulo: Atlas.
12. Jesus V (2016) Computer Forensic Treatise. São Paulo: Millennium.
13. Emerson W, Nogueira HV (2013) Cyber Crimes – Threats and Investigative Procedures In: 2nd (Edn.), Rio de Janeiro: Brasport.
14. Yusoff Y, Ismail R, Hassan Z (2011) Common phases of computer forensic investigation models. International Journal of Computer Science and Information Technology (IJCSIT) 3(3): 17-31.