Forensic Science International: Digital Investigation 42-43 (2022) 301481

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

# Cheap as chips: An accessible chip off acquisition method for ball grid array (BGA) integrated circuits in digital investigations

M. Hadgkiss*, S. Morris, S. Paget, A. Ventress, K. Norris

*Centre for Electronic Warfare, Information, and Cyber Security, Cranfield University, Defence Academy of the United Kingdom, Shrivenham, SN6 8LA, UK*

ARTICLE INFO

*Article history:*
Received 17 December 2021
Received in revised form
26 August 2022
Accepted 1 November 2022
Available online xxx

*Keywords:*
Chip off acquisition
Digital investigation
Integrated circuits

ABSTRACT

Chip off acquisition has steadily been used in digital investigations as an advanced data acquisition technique. This method has typically been reserved for devices where less invasive methods have been unsuccessful in data recovery. After a review of available literature, limited publications were found to define and discuss a detailed chip off methodology, especially using accessible and low-cost equipment. Therefore, demonstrating a lack of knowledge share and standardisation in this space.

This paper creates a methodology for chip off acquisition, that examiners can follow, using an array of equipment. The methodology was developed using accessible resources in a variety of formats and experimental research. Once constructed the method was tested in a collection of scenarios and utilised in research and consultancy. This demonstrated areas where the method was positively implemented and areas where updates could improve the overall success of the methodology. Following the evaluation, a 6-stage process was formulated: deconstruction, identification, removal, restoration, determine and perform.

© 2022 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

## 1. Introduction

As the field of digital forensics has grown over the past decade it has become an integral form of investigation. Since its inception there have been various iterations of guidance and standards, to aid examiners. The most longstanding guidance is the Association of Chief Police Officers (ACPO), Good Practice Guide for Digital Evidence, which introduced four key principles when working with digital data (Association of Chief Police Officers, 2012). This was recently followed by the introduction of ISO 17025 accreditation for digital forensics laboratories in the UK. Both set out guidelines and regulations for examiners to follow throughout an investigation, ultimately ensuring best practices and standardisation across the field. However, due to the disparity in methods and practices across organisations and examiners, their introduction is not always viewed positively.

One of the crucial stages of digital investigation governed by these standards and guidelines is data acquisition. This is the action of generating a copy of the storage media in a controlled manner and maintaining its integrity. Data acquisition can be achieved by various methods depending on the individual device and surrounding case factors. These methods are often expressed in levels, with each stage having increasing invasiveness, expense, and technically challenging components. A popular diagram to display this was created by the National Institute of Standards and Technology (NIST) shown in Fig. 1.

Due to their universal and common usage, there has been expansive coverage of the least invasive methods of investigation, including manual, and logical. Rendering highly invasive methods like chip off and micro read, that are limited to opportunities and cases that require it, with little coverage. However, the introduction of smart technology with onboard storage with limited data transfer connections has required the use of more invasive acquisition methods. All to prevent potential data changes and integrity that can occur when using these less invasive options.

Organisations have capitalised on the increased use of these methods, which has resulted in a dense market of chip off and JTAG intensive training courses. This has created an almost closed area of expertise with limited open knowledge sharing in the field. Meaning examiners are implementing these methods with a degree of variance depending on expertise, tools, and funds, like many other practices in the field. All of which support the introduction of guidelines or recognised frameworks to try and create a level of standardisation within the field.

* Corresponding author.
*E-mail address:* m.hadgkiss@cranfield.ac.uk (M. Hadgkiss).

https://doi.org/10.1016/j.fsidi.2022.301481
2666-2817/© 2022 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

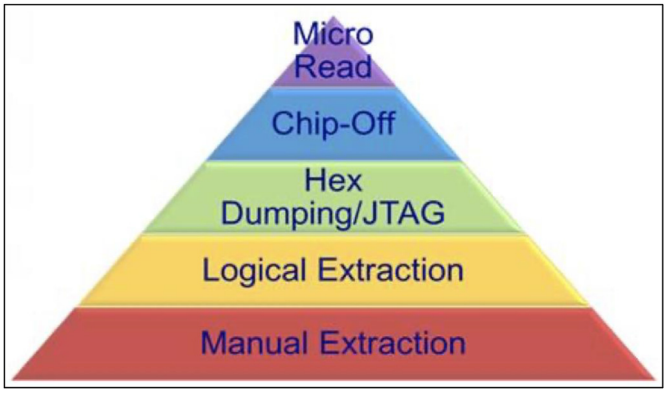



**Fig. 1.** Acquisition methods (National Institute of Standards and Technology, 2014).

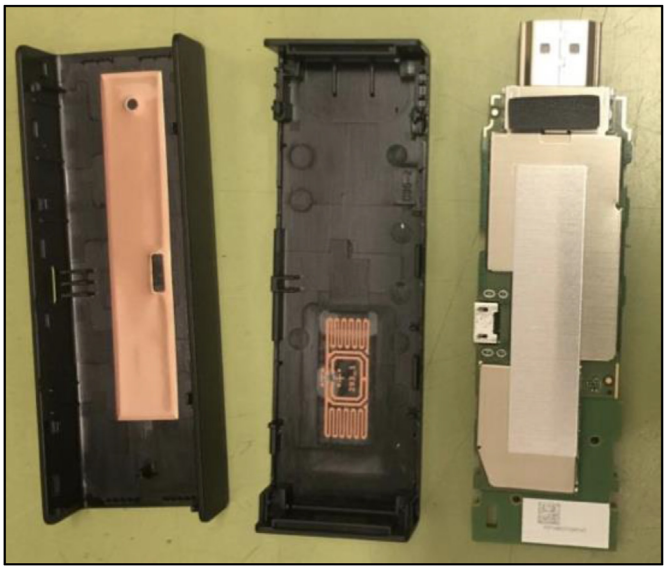


**Fig. 2.** Amazon firestick with outer casings removed.

This paper aims to create a chip off method that examiners can follow using available and accessible resources.

The remainder of this paper is as follows: Section 2 highlights the stages of device deconstruction and component restoration, Section 3 considers an overview of chip off acquisition and previous research, Section 4 examines chip off case studies, Section 5 covers the construction of the chip off methodology, Section 6 discusses the findings and Section 7 focuses on conclusions.

## 2. Device deconstruction and component restoration

When dealing with devices examiners are exposed to various electronics components and practices. This is especially prevalent in device acquisition and heavily seen in more invasive methods. As electronics components are fragile and damage can be detrimental to data recovery, any action needs to be approached with caution. Therefore, requiring examiners to have some prior understanding or practice before executing these methods.

### 2.1. Removal of casings

During the acquisition stage, a device can often require some form of deconstruction. Which often involves removing the outer casings to reveal the internal components. Outer casings can be formed from many materials. Typically, devices utilise plastic or metallic materials. However, with the increasing boom of smart devices like fridges and washing machines there has been an expansion of different materials and combinations of mixed materials i.e., glass and wood.

The first step in the removal of casings is to identify the possible opening methods of the outer casing i.e., screws, slide doors, clip openings, etc. This may be hard to identify on smaller devices due to the reduced scale, but also equally challenging on larger devices due to their vast size. A further increased difficulty is seen in devices that have permanently fixed casings with welds, adhesives, seals, etc.

To prevent any potential damage to the devices and their storage media, examiners can use test or replica devices to practice the optimum approach without risking the actual device. To acquire test devices any identifiable features e.g., names, serial numbers, model numbers, and identification marks should be noted from the exhibit. These findings can be used to construct online searches or retailer enquiries to obtain exact or similar devices. If none or limited identifying features are identified, searches can be constructed using a basic description of the device and its functionality. Image searches may be most useful in this case.

If it is difficult to procure a device, i.e., vintage, end of life, etc. examiners can use web resources to aid removal. This can include videos and web pages of devices being deconstructed.

### 2.2. Exposing of components

Once a device casing has been removed the inner electronic components are revealed (see Fig. 2). Typically, this will expose single or multiple printed circuit boards (PCB). Their purpose is to provide support and electrically connect components (Eurocircuits, 2021). It is often covered with a green solder mask, as shown in Fig. 3, giving examiners an easily identifiable quality.

Sometimes PCB's can be covered with electromagnetic interference (EMI) shields, commonly known as “cans” to protect the components from external interference or prevent signals from leaking and interfering with surrounding electronics (Moore, 2021). The shields are typically thin sheets of metallic material connected to the PCB using solder. Shields, when used on PCB's, are often covering components of interest and therefore removal is required. Removal of the shields can be completed by applying a heat source to the PCB to melt the connective solder. However, this subjects the PCB to additional heat. A less invasive method can be

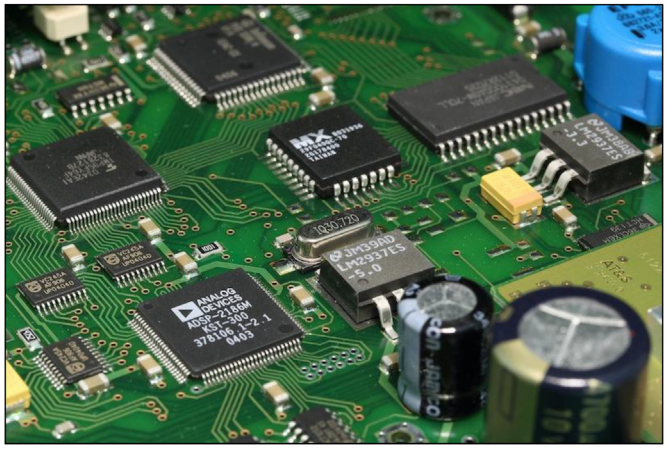


**Fig. 3.** Printed circuit board (Robotics & Automation, 2021).

employed by filing the shield's top layer, focusing on the joints of the metallic material. The shield can then be removed using tweezers and will expose the underlying components. There can be numerous shields present on the PCB and therefore an investigator may have to remove more than one, before identifying a component of interest.

#### 2.2.1. Integrated circuits

As discussed in section 3.2 and shown in Fig. 3, many electronic components can be present on a PCB. Common electronic components can include resistors, capacitors, integrated circuits (IC), and diodes. These components can take many sizes, shapes, and colours but often take a specific form for their function. Components are often mounted to the surface of the PCB or in manufactured holes in the PCB.

The main component of interest, ICs can be utilised to perform many functions, one of which is data storage, typically seen in smart and mobile devices. ICs can come in many different package types, as shown in Fig. 4, so can cause difficulty when trying to identify them on a PCB. However, ICs commonly have a black outer casing, but can sometimes take other colours, which typically makes them stand out against the green PCB.

This research focused on a popular form of ICs, ball grid array (BGA), which are ICs that use balls of solder on the underside of the package to connect to the PCB, as shown in Fig. 4. BGA ICs can have a variety of sizes and pad counts depending on their functionality, which is an integral characteristic when trying to communicate with the IC.

### 2.3. Identify components of interest

Once the PCB components have been revealed, examiners can start to identify the components of interest. As discussed in section 3.2 the component of interest is most often ICs. They typically have visual marks and qualities that can assist the investigator in identification, however, they are not always guaranteed to be there or can be obfuscated. This can make the identification of the data storage IC challenging, as there are typically numerous ICs present on the PCB.

On the face of the IC, there can often be visual clues to assist with identifying the IC of interest. These include identification numbers, manufacturer/brand names, and logos. As ICs are small components it can be challenging to display all the information on the surface, so manufacturers may employ shortening techniques to condense this information. Internet searches can be conducted using the visual clues identified to locate the manufacturer in the first instance.

After the manufacturer of the IC has been identified, the associate website or information storage can be consulted and checked for an IC search function. This sometimes will show if shorten methods have been applied and how to convert them to longer forms. Examiners can then input the identification numbers to retrieve the datasheet for the associated IC. Once retrieved the datasheet will contain all the required information to identify the ICs functionality and confirm the number of pads present on the IC and their function, which is essential for communicating with the IC.

The datasheet may not always be present directly on the manufacturer's websites, so general searching and forums should also be consulted. If there are no obvious visual clues or parts of the information are missing a brute force approach could be applied. This could involve conducting a range of searches using the information present, in hope of retrieving the information of interest.

### 2.4. Removal of components

Once the component(s) of interest has been identified, examiners can begin removing components from the PCB. Most components are attached to a PCB with solder, forming a permanent connective joint. To break the connection, the solder is heated until it liquefies allowing for easy removal without causing damage. Several tools can achieve this, the most used are hot air tools. Cheap, accessible options include a general-purpose hot air gun, which gives examiners variable heat control. More expensive options include hot air rework stations that have more accurate heat options. Once the solder is in liquid form, components can be removed from the board, this can be achieved by a range of tools. Blades and scalpels are typically the tools of choice as they provide flexibility and the ability to slide between the PCB and components. However, can cause extensive damage if they are used when the solder isn't completely liquified. This is often hard to establish due to the solder being present on the underside of the IC. Tweezers can also be utilised to lift components off the PCB but like scalpels, damage can easily occur. An alternative option is suction tools, as they only allow removal once the component is ready to be removed i.e., solder is fully liquefied. Therefore, lowering the chance of damage to the components compared to both scalpels and tweezers.

As the removal stage involves heat that can be highly damaging to components, there are various challenges throughout the stage.

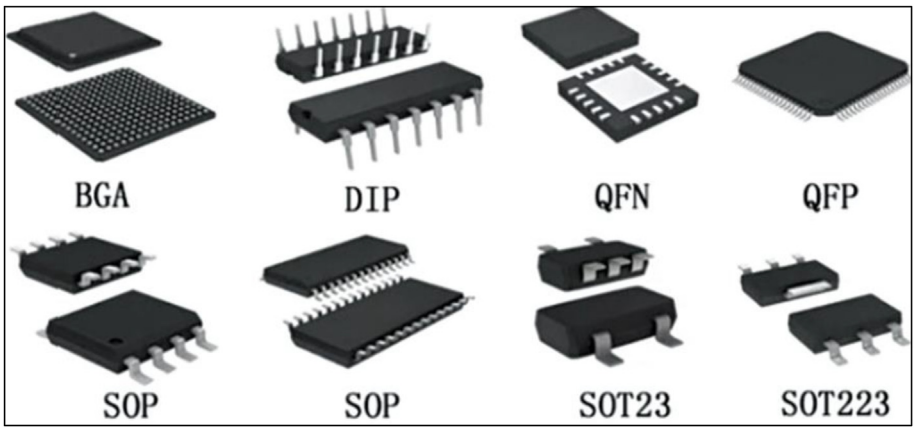



**Fig. 4.** Integrated circuit package types (Electronicsforu, 2019).

Isolation methods can be used to limit heat exposure and damage to the board and other components. One example is heat-resistant tape. This can be secured to the PCB covering the remaining components but cut to expose the IC for removal.

Another complication when removing components is adhesives and sealants. Some manufacturers are increasingly using adhesives to secure components to PCB's, in addition to solder. The adhesives can be placed discretely on the underneath components, which increases the difficulty of removal. Sometimes this means components can be subject to intensive heat when trying to remove them. Solvents can often be applied to assist with removal.

A further challenge when working with heat is temperature control. Too low and the solder will not fully liquefy, which causes an increased risk of physical component damage when attempting to remove it. Too hot and there is an increased risk of component functionality damage. Therefore, continually monitoring the heat when performing the method is essential.

### 2.5. Restoring components

When components are removed, they may require restorative work. This involves cleaning up the components and removing traces of solder and adhesives from the removal stage. This can be achieved by passing a soldering iron and solder wick over the components and collecting the solder remnants. Flux can be applied to aid and ease the process. Once the solder has been removed an alcohol cleaner e.g., isopropanol can be used to remove any last remaining contaminants. If required, afterwards a small amount of solder can be placed on the IC pads.

## 3. Chip off acquisition

### 3.1. Overview

Chip off acquisition is the complex process of physically removing a data storage IC from a PCB. Once removed specialist readers or custom PCBs can be used to extract the data. The method results in a physical alteration of the device but should prevent any changes and lead to a physical acquisition of the storage media.

### 3.2. Previous research

Chip off has been an explored acquisition method for the past decade, with a variety of publicised available information. Initially investigated by Breeuwsma et al. which noted a general method of data recovery of flash memory in digital investigations, including coverage of flash storage principles and various ways to recover data. The paper included an overview of methodologies for IC removal using hot air and universal sockets/adapters for reading (Breeuwsma et al., 2007). This provided a great introduction to chip off acquisition for digital investigations, however, lacked detailed methodology instructions, as the focus was a general overview. Furthermore, since the initial publication of this paper, there have been great advances in technology, including progress in chip off acquisition tools and techniques. Due to the increase in use since it was utilised.

After the publication of this paper, many articles went on to demonstrate the benefits of chip off acquisition, especially in the mobile device sphere. Most articles published focussed on exploring some of the acquisition methodologies for mobile device acquisition rather than concentrating on chip off acquisition (Alghafli et al., 2012) (Lohiya et al., 2015). Both again included brief coverage of a general chip off methodology and potential challenges. However, not enough to ensure repeatability for examiners as there were differences in each of the approaches.

As chip off started to be utilised far more in digital investigations, research continued and started to focus on BGA ICs, as they were now the most common IC used in electronics. Again, high-level overviews of chip off acquisition methods were used. More advanced removal techniques were also experimented with. Some looked at removing the PCB substrate and leaving the IC in situ. This was possible by using a milling machine to precisely remove material layer by layer until the BGA grid balls are accessible (Billard et al., 2015). This provided a comprehensive methodology, however, was reliant on a milling machine. Which aren't accessible or cost-effective for every examiner, therefore don't fit the requirements for this methodology.

The popularity of chip off acquisition and the ever-growing need for standard practice sparked a further study on a framework to acquire and extract data from flash memory ICs (Sansurooah, 2015). What is understood from the abstract is that a series of chip off acquisition experiments were conducted in line with the current guidelines at the time. From this, a framework was constructed for examiners to follow when working with flash memory. The only flaw of this is only the abstract is visible to examiners, as the work is restricted with no scope for access. Meaning the research cannot be practically used and validated in the field.

Researchers have also explored constructing a focused chip off acquisition method in an MSc thesis project. The output formed steps to successfully remove ICs, however, was constructed solely for the Microsoft Lumia mobile phone (Juniper, 2017). Therefore, focused on tools and methods that were most suited to that device. Thus, again creating a gap for a more generalised and accessible method to be developed.

### 3.3. Training courses

A very densely populated area in chip off acquisition is training courses, with many vendors and training providers facilitating some form of offering. These training courses are often heavily monetised and only offer a limited overview of methodologies used before the course. They also offer a form of certification or test for examiners. Thereby encouraging participants to attend to gain the knowledge and formal certification for supporting evidence in cases. Yet, with limited force budgets, understaffing and backlog pressures, it is not always easy, nor feasible for examiners to complete these courses.

As with each of the courses, there is also a degree of variance in the training, as most have different target audiences. Some will focus on a basic chip off method (Teeltech, 2021), others will focus on flash memory theory in addition to chip off (H-11 Digital Forensics, 2021), and a number will cover advanced removal techniques like subtraction (Cellebrite, 2021). This can create a disparity in experience as each will cover different techniques, at different durations, different levels of competency and content may not be delivered exactly as advertised. Meaning it's harder to interpret the value of each certification and what knowledge examiners gain.

### 3.4. Data recovery businesses

The benefits of chip off acquisition are widely recognised across various sectors including data recovery. This has especially seen a rise due to the increasing use of primary mobile devices for consumers. However, as these devices are portable, they usually suffer from some form of damage or dysfunction, often leaving consumers seeking professional assistance for data recovery.

Most mobile devices today typically use flash memory storage, thereby allowing chip off methods to be utilised for data recovery. This has created a jump in companies offering chip off data recovery offerings. Often very transparent about the process giving

detailed explanations (Gillware, 2021) and providing additional content like videos demonstrating practices (FlashFixers, 2017). This provides a great insight into practices, however, the methods displayed are often suited to their available tools and knowledge, therefore, not suitable, or accessible for all examiners. Furthermore, these services typically do not follow the required guidelines or standards for digital investigations i.e., write protection and contemptuous notes. As these services are not designed to be used in legal environments. However, they do provide examiners with options to seek alternative services if in-house expertise is not available.

## 4. Constructing a chip off acquisition method

Whilst there is a variety of available information present on chip off acquisition highlighted in section 3, it was evident that there was no recognised standard method. This provoked the development of an accessible method for all examiners. That is achieved by forming a generalised methodology using clear and concise steps that could be easily followed by any examiner.

The development stage consisted of compiling all the information discovered in section 3 to create a base methodology. This consisted of academic journals, blogs, videos and advice from electronic engineers. Each stage of the methodology was physically tested using repurposed equipment. This allowed for the assessment of the practical viability in the field, alongside what was theoretically possible.

The developed methodology was split into 6 key stages: deconstruction, identification, removal, restoration, determination and performing data recovery, which is expanded in the below sections and Fig. 5.

Once the initial method was developed it was tested on a variety of case studies to evaluate its true viability and rate of success (see Fig. 6). These cases highlighted areas in which the method worked well and places where improvements were necessary. The improvements identified were then incorporated into the final methodology.

### 4.1. Case studies

Many case studies were considered throughout the development phase. Two case studies of significance to the methodology

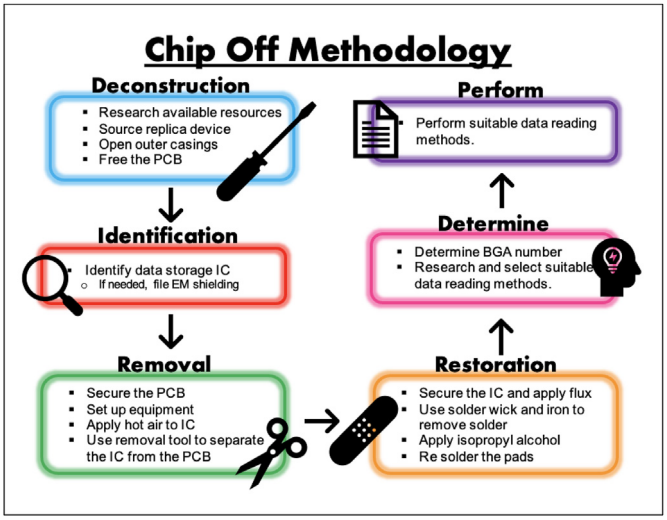



**Fig. 5.** Chip off acquisition methodology.

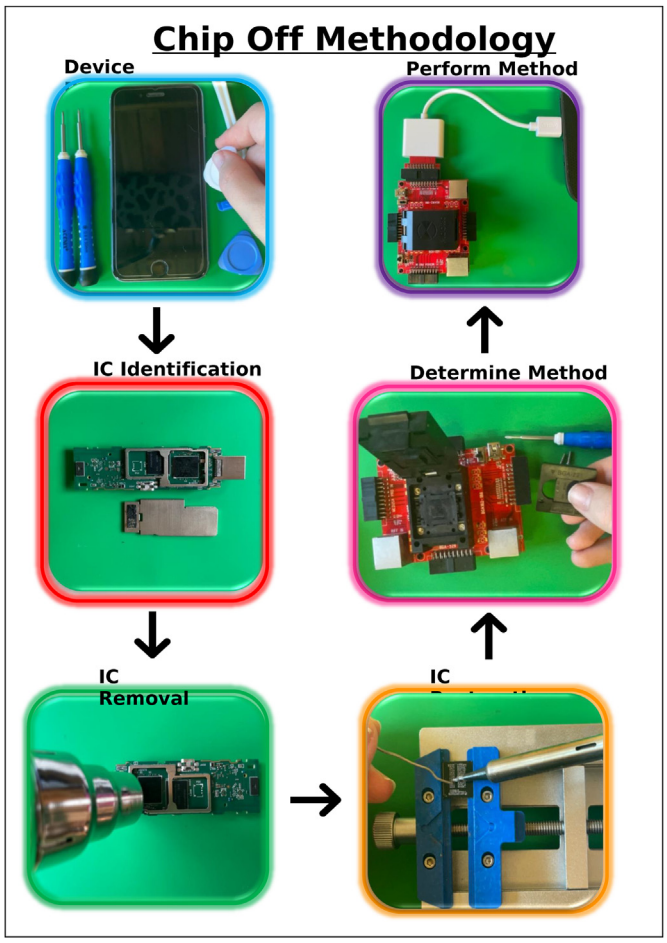



**Fig. 6.** Chip off methodology implementation images.

are featured in this paper in sections 4.1.1 and 4.1.2. Both highlighted the physical vulnerabilities of ICs and the unpredictability of working with electronics. Throughout the case studies, various pieces of low-cost equipment were used to evaluate the method. The equipment for each stage is outlined in Table 1 below.

#### 4.1.1. Operation Snappy

Operation Snappy was a case that involved the recovery of data from a damaged smartphone that didn't properly function. Commercial and open-source acquisition tools were initially tested to assess the extent of the damage. However, neither produced a sufficient connection to allow data acquisition. Leaving only more invasive options to attempt.

*4.1.1.1. Deconstruction.* The smartphone was deconstructed using a set of screwdrivers to remove screws and plastic pry tools to open the outer casing. This exposed the smartphone's PCB. Due to the tool materials used, there were no marks or scratches on the outer casing after levering apart.

*4.1.1.2. Identification.* The PCB was examined, and it was noted there were several surface mount ICs. The IC identification numbers were still visible and could be used to construct web searches. This allowed the IC datasheets to be obtained, reviewed and the storage IC to be identified.

*4.1.1.3. Removal.* The developed methodology worked well in the

**Table 1**
Table of equipment.

| Stage | Equipment |
|---|---|
| **Deconstruction** | Plastic pry tools |
| | Screwdrivers |
| **Identification** | Small metal file |
| | Tweezers |
| **Removal** | Hot air gun |
| | Thermometer/thermocouple |
| | Scalpel or blade |
| | Anti-static mat |
| | Clamps or PCB holder |
| **Restoration** | Soldering iron |
| | Solder |
| | Solder wick |
| | Flux |
| | Isopropyl alcohol |
| | Cotton bud/chamois applicator |
| **Determine Data Recovery** | Datasheet if available |
| | Vernier callipers or other appropriate measurement tools |
| **Perform Data Recovery** | BGA adapter |
| | Acquisition PC |
| | Flasher box |
| | Write-blocker |

removal stage leading to the successful removal of the IC. A heat gun was utilised at 215 °C and was constantly measured with a thermocouple. It was applied to the PCB and IC with a clearance of 1CM. When the solder was visibly molten a suction tool was applied to the IC and the IC was removed. Due to this method of removal, there was limited surface damage, meaning the IC was ready for the restoration stage.

*4.1.1.4. Restoration.* To commence the restoration stage, the IC was secured into a vice to allow for easy clean-up. A piece of blank circuit board was used as a gripping material and a secure base plate between the vice and IC. As the vice was being slowly tightened, the base plate was too narrow, and the vice slightly nipped the IC. As soon as this occurred the IC instantly split into two, causing a catastrophic failure. Once an IC is cracked or split, data recovery is near impossible due to its complex nanostructure. The case was then suspended at this stage, with no progression to data recovery.

*4.1.1.5. Case review.* This case highlighted the fragility of ICs and how one wrong move throughout the process can prevent any chance of data recovery. This failure led to the further development of the restoration stage. Any base plates used were measured to ensure that there was enough clearance between the vice and IC and standard base plates were created for popular IC sizes.

*4.1.2. Operation Stuck On You*

Operation Stuck On You was an investigation of a smart home device. At the current time, there was limited acquisition support in commercial and third-party tools. This coupled with limited data ports and non-removable storage media, meaning only invasive methods could be explored.

*4.1.2.1. Deconstruction.* Before the device was deconstructed various online videos were viewed showing how to deconstruct the device. This allowed the team to construct a suitable method to take the device apart limiting any damage. Following the adoption of the method, the smart home device was deconstructed using screwdrivers and plastic pry tools to reveal the PCB. Due to the tool materials used, there were no marks or scratches on the outer casing after levering apart.

*4.1.2.2. Identification.* The PCB was examined, and it was noted there were several surface mount ICs. The IC identification numbers were still visible and could be used to construct web searches. This allowed the IC datasheets to be obtained, reviewed and the storage IC to be identified.

*4.1.2.3. Removal.* Following the identification of the IC of interest, the board was secured in place and the heat gun was set to 215 °C and was monitored using a thermocouple. After the heat was applied to the PCB for several minutes the solder was still not molten, therefore the temperature had to be increased. The solder eventually began to turn molten at 275 °C. The suction tool was applied to the centre of the IC and a lift was attempted. However, the IC didn't shift and was still secured to the PCB. This was unsuccessfully repeated several times. The temperature was raised further up to 300 °C, and the same method was applied with no difference. A scalpel was then used to pry the IC off the PCB. With the heat applied, it was able to pass under the outer sides of the IC with ease but was unable to fully release it from the board. The scalpel was then continually passed under the IC until it was released from the PCB. Once the IC was removed it was noted that it was secured to the PCB with some form of adhesive or resin.

*4.1.2.4. Restoration.* The IC was secured to the workbench using a vice and baseplate. Firstly, any remaining adhesive was removed from the IC using a solvent and chamois tipped swab. A liquid flux was then applied to the surface of the IC and a soldering iron with solder wick was used in a sweeping motion to remove any excess solder. A chamois swab with a small amount of isopropyl was then used to remove any residues. Once the chip was cleaned it was noted that several pads had been damaged on the IC. This was most likely due to excessive pressure on the scalpel and forcing the IC off the PCB with the adhesive still present. A small amount of solder was then applied to the IC pads.

**Table 2**
Case study comparison.

| Stage | Operation Snappy | Operation Stuck On You |
|---|---|---|
| **Deconstruction** | Successful | Successful |
| **Identification** | Successful | Successful |
| **Removal** | Successful | Unsuccessful<br>• IC pads were destroyed due to the improper removal caused by adhesives. |
| **Restoration** | Unsuccessful<br>• IC snapped due to insufficient support. | Successful |
| **Determine Data Recovery** | N/A | Successful |
| **Perform Data Recovery** | N/A | Unsuccessful<br>• IC data could not be recovered due to destroyed pads. |

*4.1.2.5. Determine data recovery.* Using the available datasheet, the IC was identified as a BGA 221 eMMC. An in-house eMMC IC adapter was identified as a suitable method of connection.

*4.1.2.6. Perform data recovery.* The IC holder was set up with the appropriate size securing plate and fixed to the adapter using the 221 slot. The IC was then placed in the holder and connected to the examination machine using a USB Tableau Write blocker. No volume or storage media was identified after the connection. This was verified by using different operating systems and software. The IC behaviour in conjunction with the observed damage led us to believe that there had been some form of damage to a required pin.

*4.1.2.7. Case review.* This case highlighted the difficulties that can occur when adhesives and to be cautious of them being present on any device. In cases when adhesives are suspected before and during the removal stage, only the suction tool is utilised, to limit any potential damage. Solvents and chemical adhesive removers could also be utilised to avoid extreme heat on the IC.

## 5. Chip off methodology

Following the implementation of the adaptations identified in the case study testing, the final methodology was created. The initial 6 stages remained, with upgraded protocols and equipment, an overview is displayed in Fig. 5.

As with any evidentiary method, best practice is to ensure that the examiner is competent and able to perform activities, without cause of damage or change in evidence integrity. As chip off is a complex procedure, extra precautions are necessary. It is recommended that the examiner attempts this method on similar test devices, allowing for suitable practice before performing the method on the evidence.

Test devices can be obtained using the method described in Section 2.1. To maintain evidence integrity, a known verified device or IC could be utilised to confirm and verify the method outcomes and findings. If an examiner does not feel confident or competent in following this methodology, it should not be conducted.

### 5.1. Deconstruction

The deconstruction stage aims to strip down the device to its PCB.

#### 5.1.1. Deconstruction method

1) Check the device is ready for deconstruction to commence.
   a) Ensure that any required traditional forensics work i.e., fingerprinting and DNA extraction is completed before starting the chip off method.
   b) Assess the device and identify any potential signs of contamination and if required complete necessary decontamination steps.
2) Assess the device for signs of tampering or use of tamperproof methods.
   a) Examine the outer casing for signs of tampering i.e., marks, broken seals
      i) If possible signs are identified, construct a method to mitigate the effects of potential damages.
      ii) Identify any use of tamperproof methods i.e., specialised screws,
3) Research external sources i.e., web searches, to see if any available resources show how to deconstruct the device.
   a) If no external sources can be identified, a replica device if available should be used. This will allow for a practice deconstruction before the original device.
   b) If a replica device cannot be procured, similar devices can be investigated. A last resort option would be to move on to step 5. However, this can be very destructive, approach with caution.
4) Collate all information found to create a step-by-step process to deconstruct the device.
5) Identify the opening mechanism of the outer casing.
   a) Look for joining fixtures like screws, clips, rivets, etc that could indicate an opening. If information is found in step 3, use this to aid the process.
   b) If joining fixtures are identified, discover the tools required for removal.
6) Start removing the outer casing.
   a) Remove any joining fixtures identified, i.e., screws, clips, rivets etc making sure correct tools are used.
   b) If required use a plastic or metal prying tool to lever open any gaps.
   c) If the casings aren't opening with ease adhesives may have been used. Apply small amounts of hot air to the areas and continue to open the casing using a pry tool.
7) Once outer casings are detached, remove the PCB from the remaining device.
   a) Remove any fixtures securing the PCB to the remaining device, using appropriate tools.

### 5.2. Identification

The identification stage aims to identify the data storage IC.

#### 5.2.1. Identification method

1) Investigate the PCB and identify any BGA ICs
   a) Look out for the key visual characteristics:
      i) Typically, black in colour, however, can be other colours.
      ii) Often mounted flat onto the PCB.
   b) If EMI shielding is present on the PCB move on to step 2.
2) If EMI shielding is present:
   a) Use a heat source or file to remove the EMI shielding.
3) Conduct an internet search using the visible identifying features and obtain information to identify the IC.
   a) Use the visible identifying features i.e., brand names, logos, and product numbers to narrow the search.
   b) If the manufacturer name is present or identified using searches, search the manufactures product database or associated product number tools.
   c) If located via steps 3a and 3b obtain the datasheet for the IC. This should contain information regarding chip functionality, which will allow an examiner to identify the data storage chip.
   d) If no brand/product numbers are visible, or the search results in no hits employ a brute force approach. Proceed to the removal stage in section 5.3 and remove each of the BGA ICs present on the PCB.
4) Using the results from the research identify the data storage IC of interest.
5) Identify any presence of PCB coatings i.e., conformal coatings and develop a method for removal i.e., solvents.

### 5.3. Removal

The removal stage aims to remove the IC from the PCB.

#### 5.3.1. Removal method

1) Secure the PCB to the work area.
2) Remove any identified PCB coatings using an appropriate method.
3) If required, apply heat-resistant tape to the PCB, covering the remaining components and leaving the IC exposed.
4) Set the heat source to a starting temperate of 215 °C, due to it being the average melting temperature of lead-free eutectic solder.
   a) If available, use the IC datasheet to obtain maximum temperatures to prevent IC damage and data corruption.
5) If required, set up a temperature monitoring device.
6) If required, apply a small amount of flux around the IC to aid with the removal process.
7) Start to apply heat to the PCB and IC. Ensure there is the appropriate clearance for the heat source.
8) As the solder is melting, use removal tools to attempt to remove the IC
   a) If using a suction tool, apply it to the surface of the chip. Press down to secure the suction and attempt to remove it. If the IC is not removed from the PCB, continue to heat the IC and try again.
   b) If using a scalpel or blade slide the blade underneath the IC, do not attempt to lift or force the IC up. If there is any resistance the IC solder balls are not fully melted, or adhesives could be present. Continue to heat the IC and use solvents if required.
   c) If required, the heat source can be removed for a very short period before the solder re-hardens.
9) Once removed place the IC on an anti-static mat to cool.

### 5.4. Restoration

The restoration stage aims to restore the IC.

#### 5.4.1. Restoration method

1) Secure the IC to the work area.
2) If any adhesives remain on the IC use a solvent to remove them.
3) Apply flux to the IC surface.
4) Using solder wick and a soldering iron clean up and remove the previous solder.
   a) Apply a layer of solder to the wick before using it to improve the solder collection.
   b) Swipe the solder wick across the IC with the soldering iron directly on top of the wick.
   c) The solder wick should start to collect the solder.
   d) If solder isn't removed easily, apply more flux to the surface of the IC.
   e) Once the wick has several deposits of solder, get a new piece, and start step 4 again until all solder is removed.
5) Apply isopropyl alcohol to a cotton bud/chamois applicator, and swipe across the IC for a final clean.
6) Using the soldering iron and a small amount of solder, apply a thin layer of solder to each of the pads.

### 5.5. Determine data recovery

The Determine Data Recovery stage aims to determine the most appropriate data recovery method.

#### 5.5.1. Determine data recovery method

1) Determine the BGA number by counting the pins on the underside of the IC.
   a) This information can be confirmed in the IC datasheet if located in stage 1 deconstruction.
   b) BGA's can have a distinctive pattern for different numbers of pins, which can aid in determining the number of them.
2) Measure and make note of the IC dimensions.
3) Research if there are available adapters for the IC.
   a) Include pin count and sizes to determine a suitable option.
4) If no available adapters can be identified a custom board or set-up will have to be created and constructed.
   a) Use the information in the datasheet to identify the functions of the pads.
   b) Create and construct or outsource the creation of a custom PCB.

### 5.6. Perform data recovery

The Perform Data Recovery stage aims to perform the appropriate data recovery method.

#### 5.6.1. Perform data recovery method

1) Perform selected data method identified in stage 5, if an adapter is suitable:
   a) Identify the correct IC orientation for the read. This is often displayed as a triangle in the corner of the reader and IC.
   b) Place IC into the adapter.
   c) Connect the adapter to a write blocker using the USB conversion.
   d) Connect the write blocker to the acquisition computer.
   e) Use the acquisition tool of choice to acquire data.
2) If no suitable adapter was identified, and a custom PCB was selected:
   a) Connect the IC to the custom PCB using the chosen connection method
      i) If re-balling the chip,
         - Secure the IC in a clamp or holder.
         - Place the stencil on top of the underside of the IC, making both the IC and stencil pattern align.
         - When in the correct position, secure the stencil to the IC.
         - Apply solder paste to the top of the stencil and scrape away any excess.
         - Using the solder paste specification, determine the correct reflow temperature.
         - Using a heat source apply heat to the stencil. Once the balls have formed you will see the distinct silver shine.
      (a) If the balls do not form correctly, add some flux and reheat.
         - Allow to cool for 30–60 s
         - Remove the stencil carefully.
         - Align the IC underside facing down to the selected position on the custom PCB.
         - Apply a little heat to the IC to reflow the solder balls and affix them to the PCB.
         - Allow the IC to cool.
         - Connect custom PCB to a write-blocker.
         - Connect the write blocker to the acquisition computer.
         - Use the acquisition tool of choice to acquire data.
3) If IC continues to not read, investigate methods of troubleshooting.
   a) Utilise methods of magnification to enlarge the IC surface to show signs of damage or misplaced solder i.e., magnifying

glass, zoomed photograph. If available, viewing equipment like microscopes and x-ray devices can be utilised.

## 6. Discussion

This paper aimed to create an accessible chip off methodology that examiners could utilise. Through an accumulation of previous work and the development of new practices, the accessible chip off methodology was formed, as described in section 5. This was created using a range of cost-effective, accessible equipment and easy-to-follow practices.

The method was developed to be applied in the various digital investigation cases with devices that contain BGA ICs. This was completed to ensure that the method could contribute to standardised practice. At this stage in development, the current method does not consider other forms and types of ICs. However, this could be a proposed adaptation for future work on the methodology.

The tools selected throughout testing the methodology were focused on equipment that can be easily procured at a low cost. This was to demonstrate ways to make the method cost-effective and accessible to examiners. Whilst this does give great benefits, there may be perceived additional risks using inexpensive tooling. However, chip off as a method is an invasive and risky practice, that should only be utilised by experienced professionals that are confident in their approach. Therefore, this method just demonstrates that the use of cheaper alternative tooling is possible to yield the same results as more expensive options.

To evaluate the methodology, it was tested on multiple different case studies, this was to assess its viability in the field and its real-world performance, a summary of findings can be found in Table 2. Operation Snappy in section 4.1.1, explored the applicability of the method to smartphone data recovery. This case study demonstrated the successes in the deconstruction, identification, and removal stages. Each stage was completed with success with no errors, highlighting its likely effectiveness in the field. However, being a small study findings and successes are limited to the specific device and experimental conditions.

Weaknesses were first identified in the Operation Snappy Restoration stage. In this stage the IC unfortunately snapped causing a critical failure and rendering the process ineffective. This demonstrated inadequate practices and insufficient equipment, which is counterproductive for creating an accessible method. This was rectified by assessing the current stages and testing ways to improve them. In this instance, supportive plates were introduced in the updated methodology. Due to the failure, the rest of the testing could not be completed. Meaning key testing could not be completed for the determine data recovery and perform data recovery stages. Therefore, caused a limited understanding of how these stages could have performed in this instance.

Operation Stuck On You saw the application of the chip off method on a smart home device, described in section 4.1.2. The case study had successful deconstruction and identification stages. This coupled with previous findings from Operation Snappy, provided increasing evidence that the method could be effectively utilised in the field. Nevertheless, weaknesses and limitations were identified in the removal stage. The smart device had unforeseen adhesives present on the PCB and IC and created great difficulty in removal. As this was only identified after the removal of the IC, this limitation caused damage to IC and was later discovered data recovery was impossible. Following the discovery of this limitation, practices were added to the methodology to assist examiners through this stage. This includes additional steps on how to remove and work with adhesives that are present.

Even though case studies provided invaluable testing of the method, there will always be unforeseen challenges and limitations with the approach. One key limitation is that it has only been tested on a small range of devices, and therefore hasn't encompassed the vast nature of technology available. Further testing across a wide arch of devices could combat this.

Due to the complex nature of the chip off process, human errors can still occur. Whilst the methodology has been designed to limit potential damage, no methodology would be able to eliminate all human errors. These errors can be detrimental to the whole process and prevent any possible data acquisition and recovery. Therefore, examiners must ensure they are competent in their approach and have performed sufficient practice.

## 7. Conclusion

Following the collection of several resources, an open, accessible, and cost-effective chip off methodology was created. The methodology consists of 6-stages each following dedicated steps from device deconstruction to data acquisition. Throughout its development, the methodology was tested using case studies, in which some weaknesses were identified. This prompted further work and adaptations to the final methodology. However, even though this method proved successful with the performed case study testing, there will always be room for human error and scenarios where it cannot be utilised. This is due to the continual complexity and potential unpredictable nature of this procedure.

Following the development of this methodology, future research could look to creating a more expansive methodology. This would involve adapting the method to deal with other types and forms of IC. As well as other chip off methods and techniques that can enhance and adapt the procedure.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

Alghafli, K.A., Jones, A., Martin, T.A., 2012. Forensics data acquisition methods for mobile phones. In: International Conference for Internet Technology and Secured Transactions, 2012, pp. 265–269.

Association of Chief Police Officers, 2012. ACPO Good Practice Guide For Digital Evidence. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

Billard, D., Vidonne, P., 2015. Chip-off by matter subtraction: frigida via. In: Proc. 10th Int'l Conf. Systematic Approaches to Digital Forensic Engineering, pp. 19–24.

Breeuwsma, M., De Jongh, M., Klaver, C., Van Der Knijff, R., Roeloffs, M., 2007. Forensic data recovery from flash memory. Small Scale Digital Device Forensics Journal 1 (1), 1–17.

Cellebrite, 2021. Cellebrite learning center: cellebrite chip-off forensics training (CCOF) [online] Cellebritelearningcenter.com. Available at: https://www.cellebritelearningcenter.com/mod/page/view.php?id=11894. (Accessed 13 December 2021).

Electronicsforu, 2019. Types of IC [image] Available at: https://www.electronicsforu.com/resources/dip-smd-qfp-bga-ic-packages. (Accessed 12 November 2021).

Eurocircuits, 2021. What is a PCB or printed circuit board? - technical terms by eurocircuits [online] Available at: https://www.eurocircuits.com/pcb-printed-circuit-board/. (Accessed 6 December 2021).

FlashFixers, 2017. Youtube.com [online], Available at: https://www.youtube.com/watch?v=uMoVqoVuPns. (Accessed 15 December 2021).

Gillware, 2021. Chip-off digital forensics services | NAND recovery services [online] Gillware. Available at: https://www.gillware.com/phone-data-recovery-services/chip-off-forensics-services/. (Accessed 13 December 2021).

H-11 Digital Forensics, 2021. Chip-off forensics for mobile devices [online] H-11 Digital Forensics. Available at: https://h11dfs.com/certified-training/chip-off-forensics-for-mobile-devices/. (Accessed 13 December 2021).

Juniper, R., 2017. Chip-off forensic acquisition of a windows phone. http://dspace.barrington.cranfield.ac.uk/jspui/handle/123456789/2600.

Lohiya, R., John, P., Shah, P., 2015. Survey on mobile forensics. Int. J. Comput. Appl. 118 (16), 6–11.

Moore, N., 2021. EMC/EMI shielding explained | harwin [online] Harwin. Available

at: https://www.harwin.com/blog/emc-emi-shielding-explained/. (Accessed 8 December 2021).
National Institute of Standards and Technology, 2014. Guidelines on Mobile Device Forensics. National Institute of Standards and Technology.
Robotics & automation [image] Available at: https://roboticsandautomationnews.com/2020/10/12/how-to-choose-a-pcb-assembly-company/37284/—.
(Accessed 8 December 2021).
Sansurooah, K., 2015. A forensics framework and method in the acquisition and extraction of data from NAND Flash memory storage chip. https://ro.ecu.edu.au/theses/1725.
Teeltech [online] Available at: https://teeltecheurope.com/digital-forensic-training/advanced-chip-off/—. (Accessed 13 December 2021).



https://dspace.org/

# Cheap as chips: an accessible chip off acquisition method for ball grid array (BGA) integrated circuits in digital investigations

**Hadgkiss, Melissa; Morris, Sarah; Paget, Stacey; Ventress, Adrian; Norris, Karl**

**2022-12**
Elsevier
https://doi.org/10.1016/j.fsidi.2022.301481
Hadgkiss M, Morris S, Paget S, et al., (2022) Cheap as chips: an accessible chip off acquisition method for ball grid array (BGA) integrated circuits in digital investigations, Forensic Science International: Digital Investigation, Volume 42-43, October–December 2022, Article number 301481

Downloaded from a DSpace repository. https://dspace.org/