00 (2019) 1–13

Removing epoxy underfill between neighbouring components using acid for component chip-off

Th. Heckmann[a,c,d], J. P. McEvoy[b], K. Markantonakis[c], R.N. Akram[c], D. Naccache[d]

[a]*Institut de Recherche Criminelle de la Gendarmerie Nationale, Digital Forensics Department (INL), 5, boulevard de l'Hautil, 95300 Cergy-Pontoise, France*
[b]*Royal Holloway, University of London, Centre for Biomedical Sciences, School of Biological Sciences, Egham, Surrey, TW20 0EX, United Kingdom*
[c]*Royal Holloway, University of London, Information Security Group Smart card and IoT Security Centre, Egham, Surrey, TW20 0EX, United Kingdom*
[d]*Ecole normale supérieure, Information Security Group, Computer Science Department, 45, rue d'Ulm, 75230 Paris, France*

Abstract

In addition to traditional high temperature eutectic soldering, the use of underfill epoxy to glue the electronic components to the PCB (memory, CPU, cryptographic chips) has now become the norm among mobile phone manufacturers, e.g. Apple, BlackBerry and Samsung. Currently, this technique is the best solution to protect components against various mechanical stresses and improve reliability. Unfortunately, traditional techniques (chip-off or lapping) have become impossible to apply to underfilled components without destroying them or without moving peripheral electronic components. These component movements make the board unusable or require many hours of expensive repairs and specific hardware.

Acids and their use can be of interest in the digital forensics domain. Firstly, they can be used to de-capsulate the packaging of the electronic components before reading the chip (physical dump by chip-on), or to carry out reverse engineering of secure systems by micro-reading techniques of the silicon chip. Moreover, as we show in this paper, with the arrival of the latest generations of mobile phones, acid mixtures can be of interest if investigators want to use classical chip-off method (or the legal transplantation of damaged phones) for phones using underfill epoxy which cover the neighbouring components together (CPU, memory, capacitors, etc.).

This work introduces a new method called "underfill acid corrosion". The proposed process is based on the use of different mixtures of acids heated to various temperatures. We quantitatively study the influencing factors on the efficiency of acid corrosions on industrial underfill and present our results. Finally, we present our optimised process to unsolder electronic components which are glued together by an industrial high temperature underfill epoxy, without destroying the targeted electronic components and mobile phones PCB.

Keywords: Forensic Rework; Fuming Nitric Acid, Sulphuric Acid.

Introduction

It is often the case that electronic components maybe be required to be subjected to a forensic investigation. In the context of conventional operations (not damaged phone but lock by password) the investigator must simply unsolder the memory components to read it (password recovery) and then re-solder it to analyze the phone. During desoldering operations, investigators must obtain a phone that remains operational, without damaging the neighboring components. More specifically, in certain disasters (such as a bombing, an air crash or even a terrorist accident) a mobile phone can become unusable. As we have already shown in [1], investigators can resort to the transplantation of the damaged electronic components to make the phone operational again or to directly repair electronic components [2].

In some simple cases, the investigator only needs to replace the damaged electronic components with functional components taken from test phones. Of course, this principle is valid provided that the damaged components are not directly coupled with memory components that could return to default and damage the integrity of the data.

In the case of more severely damaged phones that do not implement encryption of memory data, it is necessary to perform a more complex operation of unsoldering the phone memory

Email addresses:
thibaut.heckmann@gendarmerie.interieur.gouv.fr (Th. Heckmann), James.McEvoy@rhul.ac.uk (J. P. McEvoy), K.Markantonakis@rhul.ac.uk (K. Markantonakis), R.N.Akram@rhul.ac.uk (R.N. Akram), david.naccache@ens.fr (D. Naccache)

and performing a transplant operation onto a test board. This double technique enables the investigator to recover the data in the memory.

These three examples have been fairly well mastered by forensic investigators. Unfortunately, industrial production and manufacturing now systematically uses thermal conductive glues (underfill epoxy) to fix electronic components together (memory, CPU, baseband, capacitors, etc.) and to the Printed Circuit Board (PCB). Thus, manufacturers add an adhesive, in addition to soldering with a high temperature eutectic mixture, under and on the components. As shown by numerous studies on this subject [3], this technique makes soldering more resistant to shock and temperature variations. Thus a conventional unsoldering, by chip-off or the replacement of a simple damaged capacitor, forces investigators to heat the component up to the degradation temperature of the underfill epoxy, which is about 400 °C. This high temperature entails considerable risks for the component's integrity.

In even more complex forensics cases, such as mobile phone with encryption (BlackBerry or iPhone), and in cases where the investigators have to perform a complete forensic transplant, it is not only necessary to transplant the memory, but also the processor that contains the key of the hardware encryption that encrypts the memory. As the electronic components face each other on the PCB, the solution of using the lapping technique, in order to overcome the difficulty of the underfill, is no longer applicable. Finally, in the case of Apple iPhone 7, 8 and X, transplantation is made even more complicated by the presence of many cryptographic components coupled together.

The purpose of this paper is not to show how to achieve the selection of components to be transplanted (which will be the subject of future research), but to show how to remove the thermal conductive glues, applied by manufacturers, between components.

The structure of the paper is as follows. Section one provides the classic forensic use of acids, section two provides the underfill problem and a new forensic use of acids, section three presents the materials and methods used, section four is an applied method for removing the underfill, section five is for discussion, and finally section six provides our conclusion and futher research.

1. The classic forensic use of acids

The classic use of acids in the field of forensic investigation is mainly divided into two applications. The first one is the stripping of the insulating layer of the silicon chip [4] in order to perform a micro-probing technique for the forensic reading of the memory chip. The second possible use is the stripping layer-by-layer of the silicon for applications of reverse engineering or reading (by micro-reading) the states of elementary cells of silicon [5].

1.1. Sample preparation for micro-probing

Like laser-matter interaction, acid corrosions for forensic applications aim at removing the encapsulation box from the chip to reveal the silicon chip's memory [6] (Fig. 1).

Figure 1: Silicon chip after acid corrosion [6]

The chip's insulating box is composed primarily of epoxy resin and other elements, which are mainly glass beads, alumina beads (Al_2O_3), boron nitride (BN), or aluminium nitride (AlN). Investigators are interested in creating a mixture of acids that removes the insulating box without damaging the rest of the chip (the silicon chip's memory, bonding wires, etc.).

Generally [7, 8], forensic investigators open the insulating box with a mixture of fuming nitric acid with a 100% concentration (3 volumes) and sulfuric acid (one volume) with a 100% concentration (Fig. 2). The whole is heated to 90 °C with an corrosion time that depends on the amount of resin to be removed.

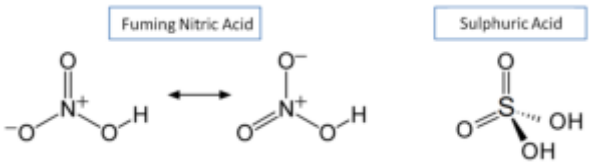


Figure 2: Nitric acid and sulphuric acid molecular patterns

For an eMMC packaging, a corrosion of 3 times 1 minute is carried out on the insulation box. A study of the fundamental chemical reactions shows that fuming nitric acid corrodes copper by:

$$4\mathrm{HNO_3}(I) + Cu(s) \longrightarrow Cu(NO_3)_2(aq) + 2H_2O(I) + 2NO_2(g)$$

and sulphuric acid corrodes aluminum by:

$$3\mathrm{H_2}SO_4 + 2Al \longrightarrow Al_2(SO_4) + 2H_2$$

Nitric acid reacts differently from sulphuric acid with metals because of the oxidizing properties of the NO_3^- radical. Thus, HNO_3^- reacting with a metal will never give rise to hydrogen H_2. Conversely, nitric acid creates a passivation layer on aluminium:

$$\mathrm{HNO_3} + Al \longrightarrow Al(NO_3)_3 + H_2O + NH_4NO_3$$

This equation shows the creation of an aluminium nitrate protective layer. In the same way, sulphuric acid protects copper with a layer of copper sulphate:

$$2\mathrm{H_2}SO_4 + Cu \longrightarrow CuSO_4 + SO_2 + 2H_2O$$

By mixing the two acids, it is then possible to take advantage of both effects by removing the resin while protecting the copper and aluminium which are present in the components (Fig. 3).

Figure 3: ENS memory chip after acid corrosion

Once the acid preparation is complete, investigators use a conventional micro-probing method to read the memory directly (physical dump). Micro-probing is used to create electrical access to a point on the silicon die or bonding wires. To establish this micrometric electrical contact, in this paper we use a probing station. Electrical contact is made by putting a micrometric needle probe directly on the silicon chip. To do this precisely, each needle is held by a micro-manipulator which is controlled by the investigator. All operations are carried out on an air-cushion table to minimise vibrations. Then voltage and current measurements are performed by the electrical measurement instruments attached to the needle probe through the micro-manipulator (e.g. oscilloscope, logic analyser, etc.), or to the investigators' homemade reader.

1.2. Sample preparation for micro-reading and reverse engineering

To remove the different layers of the silicon chip for micro-reading [9] and reverse engineering, investigators can also use the micro-lapping method. This is further illustrated Fig. 4 and covered extensively in [5].

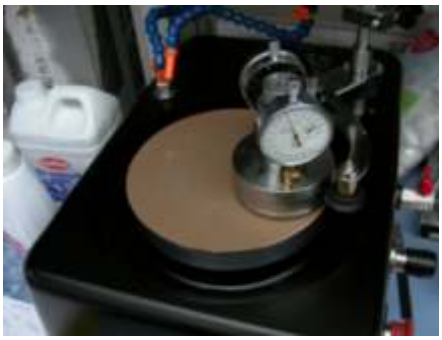


Figure 4: Cambridge lapping machine [5]

It is also possible to use different mixtures of acids in order to achieve the same effect. The chip is a juxtaposition of metals (Al, Cu, Au), dielectrics (SiO_2, Si_3N_4, BCB) and the silicon substrate. To remove the silicon oxide (dielectric), in this paper, we use hydrofluoric acid (HF) at 48% concentration or diluted in ammonium fluoride (NH_4F):

$$\mathrm{SiO_2} + 6HF \longrightarrow H_2(SiF_6) + 2H_2O$$

The acids needed to remove the metallisation layer depend on the metal. To remove the aluminium, we use a mixture of HCl + H_2SO_4 or a mixture of HNO_3 (to oxidise the aluminium) and phosphoric acid (to dissolve Al_2O_3). To remove gold, we use KI/I_2 because gold and iodine form gold-iodide via:

$$\mathrm{2Au + I_2} \longrightarrow 2AuI$$

The solubility of AuI is improved by adding KI to the solution. Therefore, to remove the copper, we use fuming HNO_3:

$$\mathrm{4HNO_3} + Cu \longrightarrow Cu(NO_3)_2 + 2H_2O + 2NO_2$$

Finally, it may be advantageous to remove the silicon substrate to carry out a backside attack.

After the Sample Preparation step, the Image Acquisition step is performed by a scanning electron microscope. The advantage of this device is its high precision and the ability to observe the memory states. Then, it is possible to read each transistor one by one (Image Processing) and use an algorithm to automate the reading process (Fig. 5).

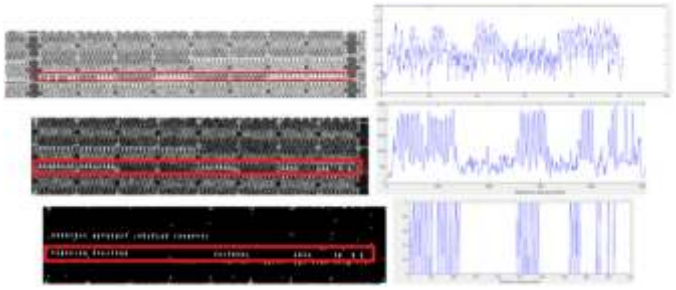


Figure 5: Cambridge 0s and 1s memory extraction using intensity values variation [5]

The layers of the memory chip are removed one by one with chemistry (or lapping or Focus Ion Beam (FIB), and then the transistors are read using the Scanning Electron Microscope (SEM) images. The step continues until all memory cells are read or totally reverse engineered.

2. The underfill problem and a new forensic use of acids

2.1. An underfill epoxy

In addition to traditional high/low temperature eutectic soldering [10], the underfill is systematically inserted in the industrial process between the electronic components and the PCB, to increase the resistance to shocks and the thermal resistance of the electronic components (Fig. 6).

Underfill has a coefficient of thermal expansion which is close to that of the eutectic solder alloy. Many papers have demonstrated an interest in the use of underfill [11] in increasing thermal and physical stress resistance (Fig. 7).

Yi He (and al.) [12] describe methods to characterise the fundamental properties using thermo-mechanical analysis, differential scanning calorimetry, and thermo-gravimetric analysis. There are several types of thermal conductive adhesives on the market, which vary according to several parameters, such as: the method of preparation (mono-component, two-component

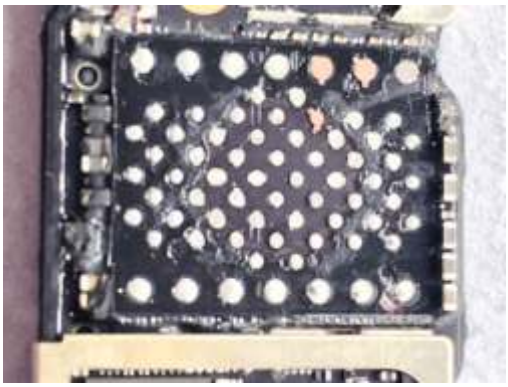


Figure 6: iPhone 7's underfill between memory and PCB

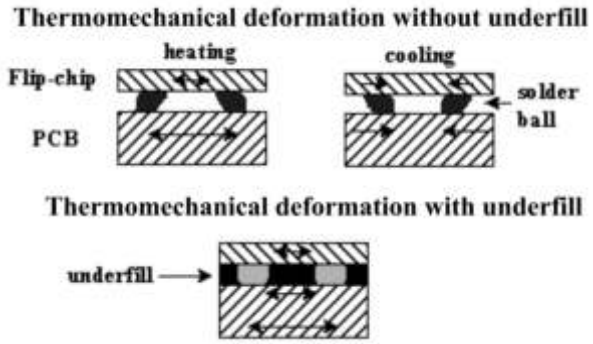


Figure 7: Thermomechanical deformation without and with underfill [3]

with resin and hardener), the coefficient of viscosity, the degradation temperature, the thermal conductivity, the Young's modulus values, the percentage of elongation at break, and the continuous resistance temperature.

Among all these different parameters, the temperature of degradation is the one that has particularly interested the investigators. Indeed, in the context of forensic operations, the investigator must heat the glue and the electronic component at this temperature in order to remove the component and subsequently perform its physical reading or transplantation.

Thus, epoxy glues with a degradation temperature of less than 300 °C are characterised by forensic investigators as low-temperature glues. The ones above 300 °C are called high-temperature epoxy glues. To guarantee a greater robustness of assembly, manufacturers now fix the electronic components close to each other, thanks to this type of glue, which also increases the density of the latest generation phones (Fig. 8).

In the case of the iPhone 7, the memory and the peripheral capacitors are fixed closely together by means of a low-temperature underfill (Fig. 9).

It is the same on the opposite face of the electronic card: the processor, the baseband co-processor as well as the peripheral capacitors are also fixed together (Fig. 10).

This overall fastening makes the assembly more robust to impact and greatly increases the resistance of the components to water. The IP Code for International Protection Marking (IEC standard 60529) is an international standard of the International Electrotechnical Commission relating to waterproofing. The

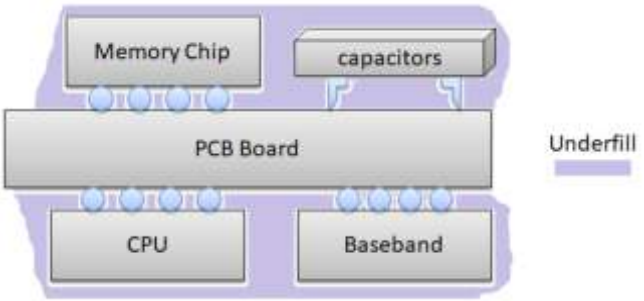


Figure 8: Underfill modeling

Figure 9: iPhone 7 memory and neighbourhood capacitors glued on board

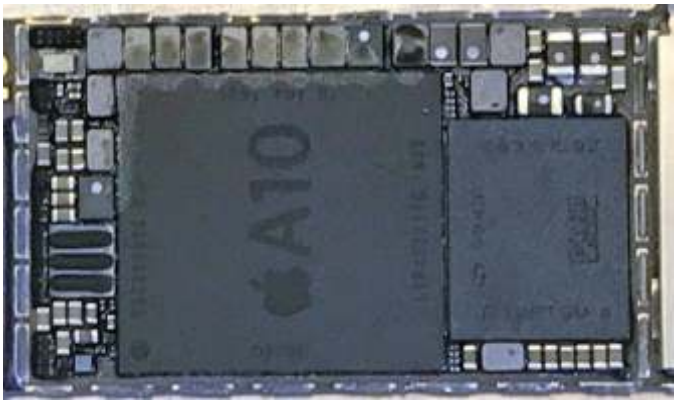


Figure 10: iPhone 7 CPU, baseband co-processor and capacitors glued together on PCB

iPhone 7, 8 and X, the Samsung Xcover 3, Android Phone D6, BlackBerry Motion, Huawei Mate 10 Pro and Google Pixel 2 have an IP rating of 67. Thus, these mobile phones can be submerged in up to 1 metre of water for 30 minutes. The Samsung Galaxy Note 8, S7 and S7 Edge, LG X Venture, HTC U11 Plus, Motorola Moto X4, LG G6 and LG V30 have an IP rating of 68. Thus, these mobile phones can be submerged in up to 1.5 metres of water for 30 minutes.

2.2. Underfill problem for forensic investigations

Investigators must now confront the widespread use of underfill in the assembly of components on an electronic card. The realisation of the chip-off technique [13] on one of these components will cause an overall movement and thus the destruction of the electronic card (Fig. 11).

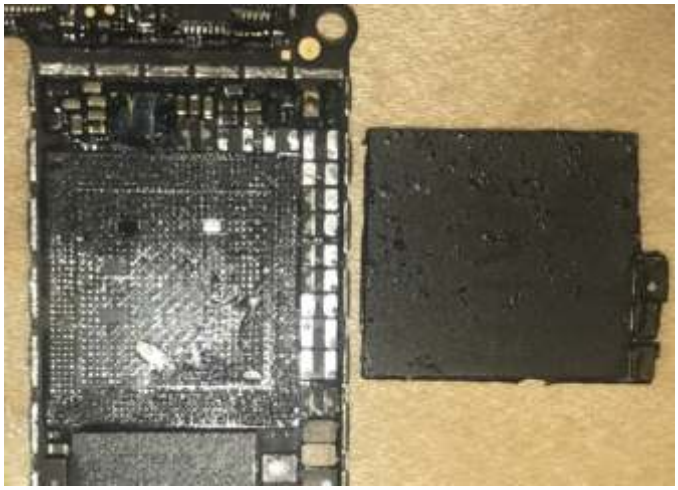


Figure 11: Destruction of the neighbourhood capacitors due to underfill on iPhone 7 CPU after classical chip-off

This overall movement is due to the fact that to remove the component, the investigator doesn't get to the degradation temperature of the glue as well as the soldering materials (BGA ball). When the investigator exerts a perpendicular mechanical force to remove the component, as is the case with the conventional chip-off method, all the components that are poured into the same block of underfill will be set in motion. These movements will create a short circuit of the other components and thus destroy the electronic card (Fig. 12).

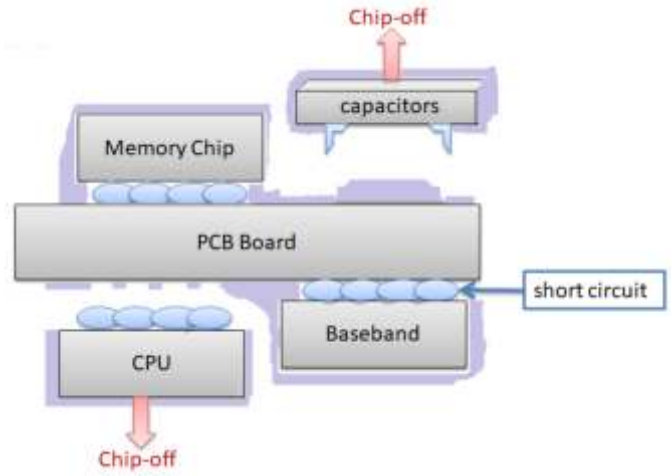


Figure 12: Destruction of the neighbourhood capacitors due to underfill after classical chip-off

Thus, techniques that were quite well-mastered until now are no longer applicable to current generations of mobile phones, even in cases in which the investigator must make a simple change of one of the electronic components. To do this, the investigator usually proceeds to replace the defective components to make the phone operational again. But basic replacement, which has become a routine technique, becomes inapplicable on underfilled phones.

2.3. The Proposed Use Acids

In this paper we propose a method to remove the underfill located between neighbouring electronic components without damaging the components and the PCB (Fig. 13).

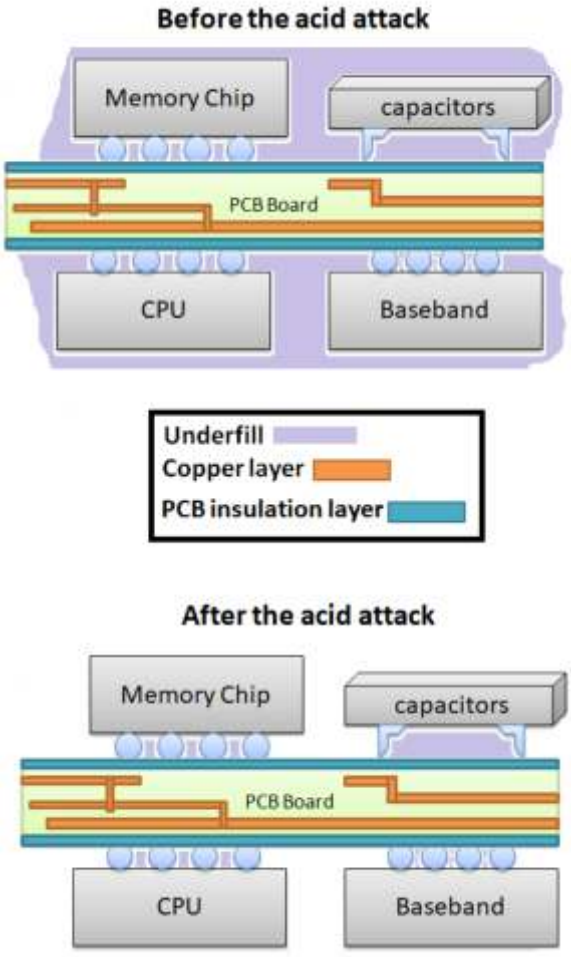


Figure 13: Theoretical result expected after chemical corrosion

The main idea behind this paper was to select acid mixtures able to remove the underfill without damaging the components, and to minimise the damage to the layers of the PCB. We have already noted that mixtures of different acids create layers of passivisation that can protect materials that we do not want to be damaged.

All the focus of our study lies in the development and the optimisation of an acid corrosion method of the underfill without corroding the layers of the PCB and the insulating layer of the electronic components (CPU, memory, capacitors and crypto-components). The tests were therefore conducted with

different acids at different concentrations, and with mixtures of acids at different concentrations. The set of experiments also looked at the influence of the temperature of the mixtures on the ablation rate and the damage to the peripheral components.

3. Materials and methods

3.1. High temperature synthetic underfill

The Thermal Conductive Adhesive (TCA) studied in this paper (Polytec TC430 [1]) consists of two components: resin and hardener. The mixing ratio is 100 resin : 4 hardener by weight (Fig. 14). This underfill was selected because of its high temperature resistance and its high power of restitution to the thermal and physical stress. Successfully removing high temperature underfill will also remove most of the lower-resistance underfill found on current phones (iPhones, BlackBerry, etc.).

Figure 14: Resin (left), hardener (right)

The viscosity at 23 °C is 13000 mPa.s and curing time is 60 minutes at 100 °C and 15 minutes at 150 °C. The pot life at 23 °C is 2 days, which allows for making alterations. The degradation temperature is 400 °C.

The preparation of the underfil will be realized and modeled in blank tablets of medicine (Fig. 15a). The whole is then dried in an oven at 150 °C for 60 minutes (Fig. 15b).

(a) Glue in pharmaceutical packaging

(b) Oven-dried glue

Figure 15: Sample preparation

The samples are then extracted from the pharmaceutical packaging and are individually weighed as we will describe later (section 4).

3.2. Nitric acid 69%

We used nitric acid 69% AnalarR NORMAPUR® analytical reagent (Fig. 16a). The boiling point is 120.5 °C (1013 hPa) and melting point is −42 °C. Density is $1,4\ g.cm^{-3}$ at 20 °C and mass weight is 63.01 $g.mol^{-1}$.

(a) Nitric acid 69%

(b) Sulphuric acid 95%

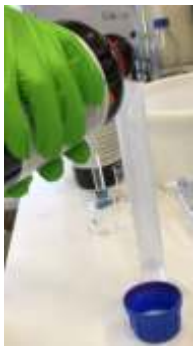
Figure 16: AnalarR NORMAPUR® analytical reagent

3.3. Sulphuric acid 95%

We used sulphuric acid 95% AnalaR NORMAPUR® analytical reagent (Fig. 16b). The boiling point is 330 °C (1013 hPa) and melting point is −10.38 °C. Density is $1,84\ g.cm^{-3}$ at 20 °C and mass weight is 98.08 $g.mol^{-1}$.

3.4. Laboratory equipment

In our experiments, we used the conventional equipment for the treatment of highly concentrated nitric and sulphuric acids (laboratory flasks and containers, Erlenmeyer flasks, graduated cylinders, adjustable-volume pipettes, etc.), as well as protective equipment (Fig. 17a).



(a) Acid mixture preparation

(b) Heating plate and Fisherbrand magnetic stirring bar

Figure 17: Acid preparation in laboratory

All the operations were carried out under a filtered atmosphere host. For heating and mixing the acids we used a heating plate and a Fisherbrand magnetic stirring bar (Fig. 17b).

[1] http://www.polytec-pt.com/

3.5. Mobile phone test board and PCB test board

In all our studies, we used both real mobile phone PCBs (iPhone 7, BlackBerry 9900, etc.) with underfill on the memory chip and CPU components, or two-level test PCBs and eMMC chip that can be obtained from low-cost electronics companies.

4. Applied method: removing the underfill

4.1. Protocol

Our tests were initially conducted with nitric acid at different concentrations. Each concentration was heated to different temperatures (Section 4.2). We then repeated the same experiments with sulphuric acid (Section 4.2). Finally, we mixed these two acids at different concentrations and temperatures (Section 4.3). The protocol was therefore identical in the three cases, namely:

- Step 1: Preparing the acid, or acid mixture, using a graduated cylinder (Figure: 18).

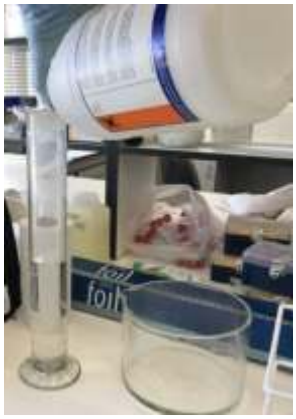


Figure 18: Step 1: preparing the acid or acid mixtures

- Step 2: Adjusting the temperature of the acid or acid mixture. The desired temperature of the acid or acid mixture is obtained by means of a heating plate and a Fisherbrand magnetic stirring bar (Fig. 19).

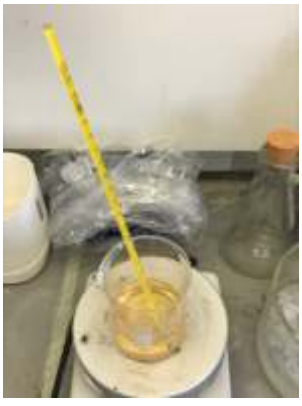


Figure 19: Step 2: adjusting the temperature of the acid or acid mixture

- Step 3: Selecting of a piece of conductive glue and weighing it (Fig. 20).

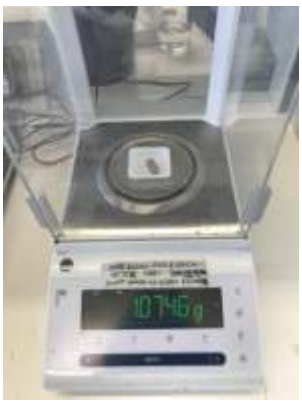


Figure 20: Step 3: weighing the selected piece of glue

- Step 4: Inserting a piece of previously weighed conductive glue in the acid or acid mixture ($Mass_{Before}$)(Fig. 21).

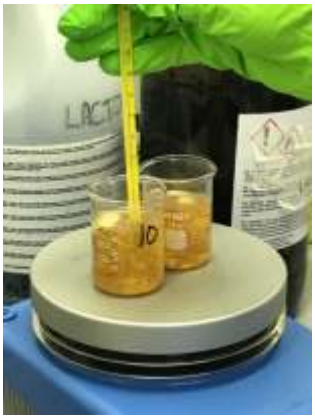


Figure 21: Step 4: inserting the glue in the acid or acid mixture

- Step 5: Removing the piece of glue after time T, called T_{attack} (Fig. 22) .

Figure 22: Step 5: removing the piece of glue after T_{attack}

- Step 6: Rinsing the piece of glue with distilled water and drying in the oven (70 °C) for 3 days (Fig. 23) .

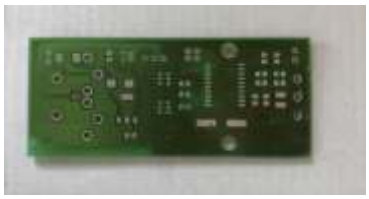
Figure 23: Piece of glue after drying.

- Step 7: Weighing the piece of glue after corrosion and after drying ($Mass_{After}$).
- Step 8: Calculating the rate of ablation:

$$\text{Rate (mg.minute}^{-1}) = \frac{Mass_{Before} - Mass_{After}}{T_{attack}} \quad (1)$$

In order to look at the effect on an electronic component and on the PCB, we corroded in the same way an eMMC chip, with underfill on the rear face (Fig. 25a) and a test piece of PCB (Fig. 24b).

(a) eMMC during corrosion



(b) PCB test piece

Figure 24: eMMC and PCB test piece

The aim of the corrosion on the memory chip is to see if the acid mixture (at a given concentration, temperature and time) damages the component. It is also to determine, in the case of corrosion, the time required for the acid to remove the layer of insulation (T_{max}) and expose the silicon, bonding wire, or first layer of copper. In the examples in figure 25, the acid corrosion was too long ($T_{attack} > T_{max}$). It certainly weakened the underfill but it damaged the protective layer until it exposed the first layer of copper (Fig. 25a) and destroyed the package (Fig. 25b).

The same principle is applied to the PCB. The key is to calculate the time needed to remove the first layer of insulation and expose the copper layer. This determination of the maximum corrosion time (T_{max}) is essential. Indeed, the corrosion on the underfill must be efficient well before the T_{max} is reached.

There are two ways to corrode the PCB. The first is to heat the PCB in an oven, then to inject onto the PCB acid heated to the same temperature on the PCB, for a time T (Fig. 26a). This operation will be the one to carry out during real corrosions on mobile phone cards.

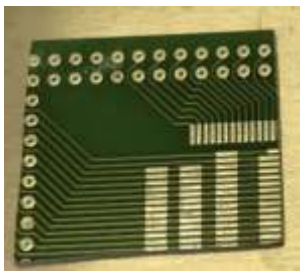
(a) eMMC with $T_{attack} = T_{max}$

(b) ($T_{attack} > T_{max}$)

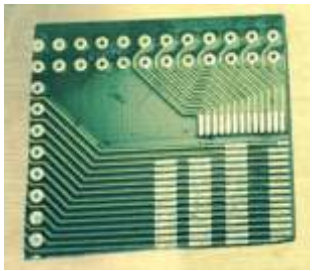
Figure 25: Memory components at different T_{attack}

The second possibility, which we have chosen in the course of our tests, is to directly submerge the PCB in an acid mixture at the desired temperature. Thus, for a corrosion at $T_{attack} = 0$ the PCB is intact (Fig. 26b). For $T_{attack} < T_{max}$, the insulating protective layer of the PCB is intact (Fig. 26c). For $T_{attack} = T_{max}$, the insulation is partially corroded, but not totally, and does not affect the copper of the first layer (Fig. 26d). The board is still operational.

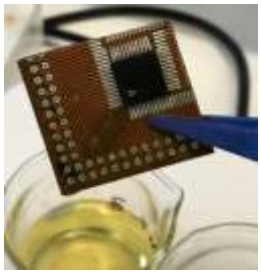
(a) PCB preparation



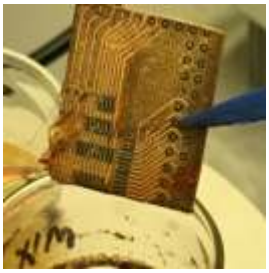
(b) $T_{attack} = 0$



(c) $T_{attack} < T_{max}$



(d) $T_{attack} = T_{max}$



(e) $T_{attack} > T_{max}$

(f) $T_{attack} >> T_{max}$

Figure 26: PCB at different T_{attack}

For $T_{attack} > T_{max}$, the first layer of copper is damaged and this damages the integrity of the PCB (Fig. 26e). The board is no longer functional. Finally, for $T_{attack} >> T_{max}$, the first layer of copper is completely corroded and the acid begins to

shrink the lower layers (Fig. 26f).

4.2. Results with sulphuric acid and nitric acid

Following the previously defined protocol, we determined the ablation rates of the synthetic underfill for 95% sulphuric acid and then with 69% nitric acid, at three different temperatures: 23 °C (ambient temperature), 70 °C and 90 °C (Fig. 27).

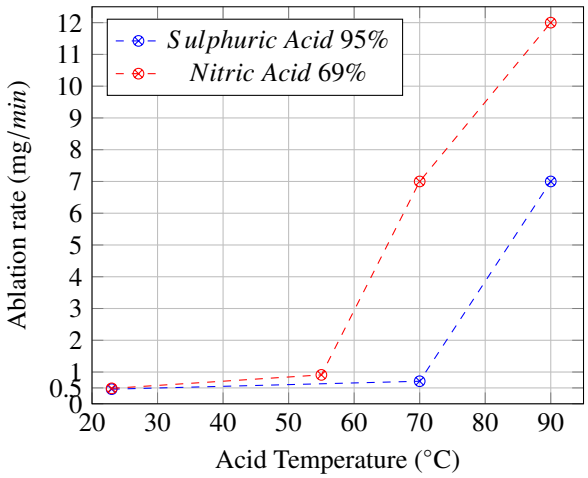


Figure 27: Results with sulphuric acid (95%) and nitric acid (69%) at various temperatures

4.3. Results with mixtures of sulphuric and nitric acids

Following the previously defined protocol, we determined the ablation rates of the synthetic underfill for a mixture of 95% sulphuric acid, three volumes, and 69% nitric acid, one volume (Fig. 28); again at the three temperatures of 23 °C (ambient temperature), 70 °C and 90 °C. We noted, however, that the mixture of nitric and sulphuric acid caused an exothermic reaction; the temperature did not remain at 23 °C, but climbed to 40 °C. Mixtures at 70 °C and 90 °C were heated to a steady temperature. We repeated the experiment with 95% sulphuric acid, one volume, and 69% nitric acid, one volume, the temperature did not remain at 23 °C, but climbed to 53 °C (Fig. 28).

We also repeated the experiment with 95% sulphuric acid, one volume, and 68% nitric acid, three volumes, but this mixture was too corrosive and damaged the electronic components and the PCB too quickly. Thus, this last mixture is not applicable to forensic applications, and is not shown in the graph.

4.4. Direct forensic applications

After characterising and quantifying the effect of acids and mixtures of acids on synthetic underfill, we performed tests on mobile phone boards. We were primarily interested in the Apple iPhone 7 and secondarily on the BlackBerry 9900.

4.4.1. Application to the Apple iPhone 7

Our results show that mixing of 95% sulphuric acid, one volume, and 69% nitric acid, one volume at a temperature of 70 °C seems a good compromise to apply to the iPhone 7, which uses a high temperature underfill.

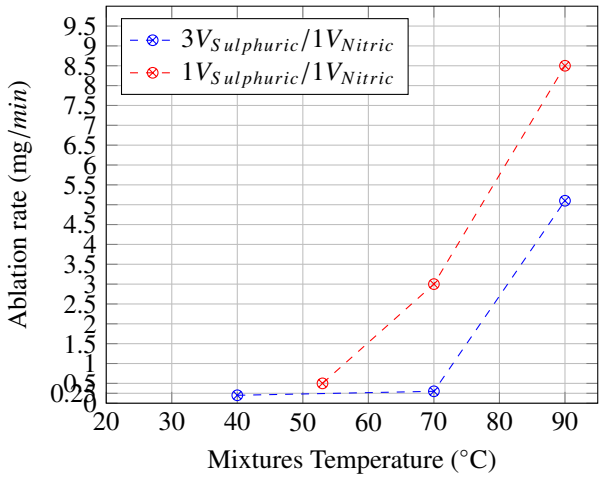


Figure 28: Results with sulphuric acid and nitric acid mixed in various proportions at different temperatures

We also determined in minutes the maximum time the acid may be applied before compromising the integrity of the electronic component ($T_{max_{component}}$) and of the PCB ($T_{max_{PCB}}$).

For corrosion exceeding $T_{max_{component}}$ the components were no longer in working order. For corrosion exceeding $T_{max_{PCB}}$, electrical tracks of the board's sublayers were destroyed.

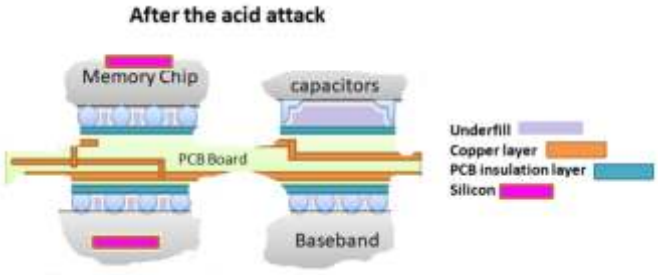


Figure 29: Result after too long chemical corrosion: components and PCB internal layers destruction ($T_{attack} > T_{max_{component}}$ and $T_{attack} > T_{max_{PCB}}$)

Then, for a corrosion application greater than $T_{max_{component}}$ and $T_{max_{PCB}}$ (Fig. 29), irreversible damage was found on both the components and the inner layers of the PCB.

We determined experimentally that for the iPhone 7 and with this acids mixture we have $T_{max_{component}}$= 360 seconds and $T_{max_{PCB}}$ = 80 seconds..

After 80 seconds of corrosion at 70 °C, the underfill present on the capacitors is sharply reduced and it loses its property of mechanical resistance. Thus, it becomes possible to remove the underfill with a micro-instrument tip (Fig. 30).

The set of neighboring components (capacitors), as well as the memory, are not damaged during the corrosion (Fig. 31). It is thus possible to cleanly remove the underfill connecting the memories and all the peripheral components. This step is necessary before desoldering the memory.

Then a conventional desoldering method is performed to confirm that the underfill is no longer present and that the peripheral components have not been moved during desoldering,

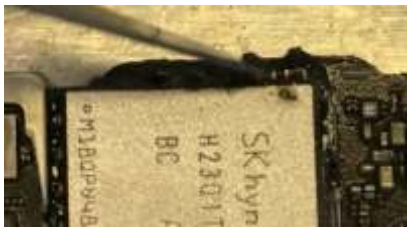


Figure 30: Easy removal of the iPhone 7 underfill after acid corrosion

Figure 31: iPhone 7 underfill after acid corrosion ($T_{attack} < T_{max}$)

which was previously the case with the underfill. To check that the peripheral capacitors have not moved during the desoldering of the memory, we perform X-ray tomography (Fig. 32).

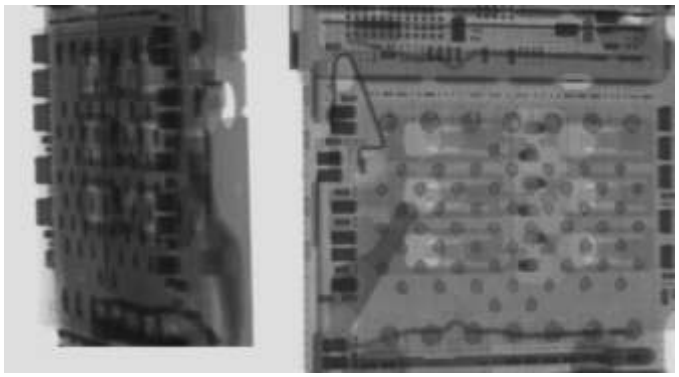


Figure 32: iPhone 7 X-ray control

The results of the tomography shows that the peripheral components have not moved, that the chemical corrosion was correctly performed, and effective enough to remove the junction underfill between components.

4.4.2. Application to the BlackBerry 9900

The BlackBerry 9900 also has underfill between components, making forensic transplantion impossible without moving nearby electronic components (Fig.33). The underfill of the BlackBerry seems more resistant to acids than the iPhone 7 and the exposure time to the acids needs to be longer, but also the acid mixture temperature.

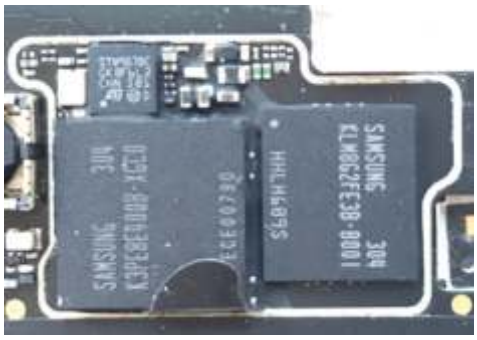


Figure 33: BlackBerry 9900 underfill between components

As the exposure time is longer, we first need to protect some elements of the board that are sensitive to acids using an acid resistant paste (see discussion and Fig. 34).

(a) Chemical protection near CPU (b) Global chemical protection

Figure 34: Setting up the chemical protection paste

Then the acid is directly applied with a pipette into the well that has been created (Fig. 35). In order not to lower the temperature of the acid during this process, the board is heated in the oven for one hour at the corrosion temperature. Our results show that mixture of 95% sulphuric acid, one volume, and 69% nitric acid, one volume at a temperature of 80 °C seems a good compromise that can be applied to on the BlackBerry 9900.

Figure 35: BlackBerry 9900: application of the acid with a pipette

After 120 seconds of corrosion, the underfill not needed on the capacitors is sharply reduced and loses its property of me-

chanical resistance. It is then also possible to remove the underfill between neighbouring components with the same process as that of the iPhone 7 previously presented.

5. Discussion

When we carried out our first tests, we totally immersed the boards of the iPhone 7 to characterise the possible damage on the electronic components and the PCB with different acid mixtures at different temperatures (Fig. 36).

Figure 36: PCB in the acid at T_0= 0 s

The mixture was allowed to work (Fig. 37a) and then washed off thoroughly with distilled water to stop the acid reaction (Fig. 37b). The board was placed in an oven for 24 hours before reassembling the phone screen, keyboard and battery.

(a) PPCB in the acid at $T > T_0$

(b) Cleaning the PCB

Figure 37: Acid corrosion and cleaning

If the phones turned on again, it was considered that the acids had not damaged the components of the phones and therefore that the maximum corrosion time was not reached. In these experiments, when the corrosion caused the phone not to start up, it was concluded that the corrosion had damaged the components or the PCB.

However, this method is not recommended for real cases and it is essential to use a localised corrosion. To do this it is advisable to protect the phone with a paste resistant to acids and easy to remove (Fig. 38) in order to decrease the risk that acid residues penetrate under or into the component. A vinylpolysiloxane paste is highly resistant to all of this acid mixtures and can be easily removed without damaging the components.

Figure 38: Vinylpolysiloxane paste

For very sensitive cases we recommend using a commercial product (Fig. 39, Shenzhen Hua Sheng Electronics CO.,LTD), which does not use acids (perfect for damaged components) but whose efficiency is greatly reduced compared to acids. This product makes it possible to soften the underfill but it will also be necessary to use, in addition, a micro-instrument to remove it physically.

Figure 39: Commercial BGA IC adhesive removing

Unfortunately, because of the viscosity, commercial products are therefore difficult to apply for small components like capacitors around the processor of the iPhone 7.

5.1. First observed limits

The first results led to the destruction of the PCBs (Fig. 40) because the corrosion times were too long, the acids too concentrated, and the temperatures of the acids were critical.

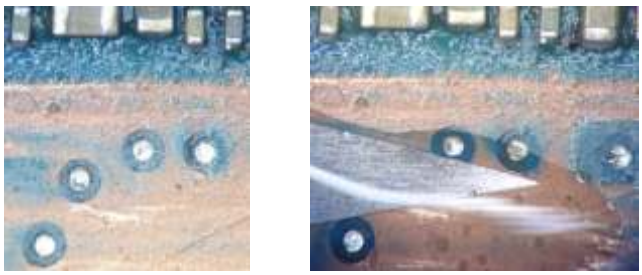
This destruction could be visible directly, but could also be difficult to detect when some small capacitors were corroded

Figure 40: Destruction ($T_{attack} > T_{max}$)

and destroyed. In addition, the acid resistance of boards that have not been previously subjected to shock, and are in perfect working order, have been characterised. But it must be remembered that a phone that suffers a shock following a crash or explosion is greatly weakened. There is therefore no advantage submerging the phone fully into acid, at the risk that acid could seep into a weakened area (fracture or crack) and continue to corrode the component (or the electronic card) from the inside, without the possibility of stopping the reaction.

5.2. Second observed limits

This paper's method and protocols allows removable of the underfill between neighbouring components. That is the first step to forensic tranplantation of encrypted and damaged mobile phones. However, the method does not allow the removal of underfill present under the component, at the level of the beads glued to the PCB. The infiltration of the acid under the component is only on the periphery and does not reach the central part. There is still some glue between the PCB and the component centrally. Thus, in some cases, desoldering results in the destruction of the first insulating layer of the PCB at the level of the central BGA balls of the electronic component (Fig. 41a).



(a) PCB insulation layer destruction after chip-off

(b) PCB insulation layer reparation

Figure 41: PCB insulation layer repair [2]

In this case, the method developed by [2] may be set up in order to artificially recreate the protective layer with an insulating resin (Fig. 41b).

5.3. Choice of acids

When testing with pure acids, 95% sulphuric acid was selected because lower concentrations are not efficient enough to work on the underfill even at high temperatures. It would have been possible to select sulphuric at a higher concentration, for better effectiveness, but it would then have been necessary to carry out the protocol again in order to be able to characterise it totally.

This principle was applied to the selection of 69% nitric acid. Concentrations greater than 69% produce too fast a reaction which would impair the integrity of the components and PCB too rapidly. However, it might be possible to select nitric acid at a lower concentration that would reduce the ablation rate, but still remain efficacious in reactions at concentrations greater than 50%. The protocols would also have to be reapplied (re-evaluated) in order to fully characterise it and better respond to the expected results.

5.4. Choice of tests on high temperature underfill

It was decided to conduct this study on high temperature underfill, rather than low temperature underfill, because the new generation of phones is using it. Indeed, the thermal protection is better and the possibilities of reverse engineering are strongly limited with the high temperature underfill. The chip-off technologies at very high temperatures have significant effects on the integrity of the data itself, and the lapping techniques become difficult on the components that face each other, as on the iPhone. Thus, for increased physical security, companies have chosen the high temperature underfill.

6. Conclusion and further research

These experiments with judiciously selected acid corrosions, allowed removal of the underfill between neighbouring components (by acid corrosion) with control and without destroying the electronic components or the circuit boards (acid passivation). This method is an evolution for classical method, like the physical grinding of underfill between the components to free them, because it allows to remove underfill onto unaccessible area by using classical micro-instruments.

The first tests were initially destructive; but as shown, several parameters can influence the efficiency and speed of acid corrosions. The first parameter of influence corresponds to the choice of acids. This choice must be made according to the target materials to be removed, and especially the materials to be preserved.

The second parameter is the choice of the concentrations of the different acids and the percentages of the mixtures. These two parameters are also highly dependent on the target materials to be preserved and ablated.

Finally, the last two parameters correspond to the choice of the temperatures of the acid mixtures, and the time of application of the acid on the target materials. This latter parameter is greatly dependent on the amount of material to be ablated and the resistance of the neighbouring elements to the acid mixtures during the total duration of application.

Thus, it is harmony between all of these parameters that makes the corrosion effective. It is therefore the result we want that will make us choose and select the most influential factor

for our application. It will also depend on the type of components to protect and the amount of material to remove. Finally, it may be possible to protect the excessively sensitive components by a deposit of acid-resistant material directly on the component and/or PCB.

The removal of the underfill is one of the first necessary steps for larger-scale forensic operations, such as the physical reading of memory by chip-off or the transplantation of mobile phones.

The success of underfill removal, without damaging neighbouring components, opens a path for the achievement of transplants of phones that have underfill (like the iPhone or BlackBerry) and whose transplantation has resulted in the destruction of the mobile phone.

Future tests are going to be conducted to implement new hardware techniques allowing quick identification of the paired cryptographic components, as it is now the case on Apple secured mobile phones.

Finally, we have not taken into account the effect of long-term use of a device on the package. We only used new and unused phones (PCBs, components). But we need to know that the composition of the package seems to change by intensive use, which is an issue in laser decapsulation and is also observed with acid decapsulation. We need now carry out serious research on this, because it seems that a fraction of harder, more brittle and more carbon-rich parts are created by prolonged times at high (like working) temperatures. As a result, the influence of acid on underfill and package of the reference telephone could deviate significantly from the final telephone PCB that is to be investigated.

Acknowledgements

The authors would like to thank Graham Houghton, for his support and contribution to this article.

References

[1] T. Heckmann, K. Markantonakis, D. Naccache, T. Souvignet, Forensic smartphone analysis using the adhesives transplantation of Package on Package components, Digital Investigation, in press, dio:10.1016/j.diin.2018.05.005 (2018) pp. 10.

[2] T. Heckmann, T. Souvignet, D. Naccache, Electrically conductive adhesives, thermally conductive adhesives and UV adhesives in data extraction forensics, Digital Investigation 21 (2017) 53 – 64. doi:http://dx.doi.org/10.1016/j.diin.2017.02.009.
URL http://www.sciencedirect.com/science/article/pii/S1742287616301347

[3] J. Okura, S. Shetty, B. Ramakrishnan, A. Dasgupta, J. Caers, T. Reinikainen, Guidelines to select underfills for flip chip on board assemblies and compliant interposers for chip scale package assemblies, Microelectronics Reliability 40 (7) (2000) 1173 – 1180. doi:https://doi.org/10.1016/S0026-2714(00)00044-5.
URL http://www.sciencedirect.com/science/article/pii/S0026271400000445

[4] O. Kömmerling, M. G. Kuhn, Design principles for tamper-resistant smartcard processors., Smartcard 99 (1999) 9–20.

[5] F. Courbon, S. Skorobogatov, C. Woods, Reverse Engineering Flash EEPROM Memories Using Scanning Electron Microscopy, Springer International Publishing, Cham, 2017, pp. 57–72. doi:10.1007/978-3-319-54669-8-4.

[6] F. Kerisit, B. Domenges, M. Obein, Comparative study on decapsulation for copper and silver wire-bonded devices, in: 40th International Symposium for Testing and Failure Analysis, ASM International, 2014, pp. 87–93.

[7] S. Murali, N. Srikanth, Acid decapsulation of epoxy molded ic packages with copper wire bonds, IEEE Transactions on Electronics Packaging Manufacturing 29 (3) (2006) 179–183.

[8] T. Lee, Mechanical and chemical decapsulation, Microelectronic Failure Analysis. Desk Reference, 3 rd Edition. ASM International, Member/Customer Service Center, Materials Park, OH 44073-0002, USA, 1993. (1993) 61–74.

[9] S. Brother, How cell phone "forensic" tools actually work-proposed leveling system., in: Mobile Forensics World, Chicago, Illinois, 2009.

[10] T. Heckmann, T. Souvignet, S. Lepeer, D. Naccache, Low-temperature low-cost 58 bismuth - 42 tin alloy forensic chip re-balling and re-soldering, Digital Investigation 19, in press. doi:http://dx.doi.org/10.1016/j.diin.2016.10.003.

[11] K. Mishiro, S. Ishikawa, M. Abe, T. Kumai, Y. Higashiguchi, K. Tsubone, Effect of the drop impact on BGA/CSP package reliability, Microelectronics Reliability 42 (1) (2002) 77 – 82. doi:https://doi.org/10.1016/S0026-2714(01)00230-X.
URL http://www.sciencedirect.com/science/article/pii/S0026271401

[12] Y. He, B. E. Moreira, A. Overson, S. H. Nakamura, C. Bider, J. F. Briscoe, Thermal characterization of an epoxy-based underfill material for flip chip packaging, Thermochimica Acta 357-358 (Supplement C) (2000) 1 – 8. doi:https://doi.org/10.1016/S0040-6031(00)00357-9.
URL http://www.sciencedirect.com/science/article/pii/S004060310

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