2015

Mobile device damage and the challenges to the modern investigator

Dan Blackman

Security Research Institute, Edith Cowan University, d.blackman0@our.ecu.edu.au

DOI: 10.4225/75/57b3fef2fb891

13th Australian Digital Forensics Conference, held from the 30 November – 2 December, 2015 (pp. 123-131), Edith Cowan University Joondalup Campus, Perth, Western Australia.

MOBILE DEVICE DAMAGE AND THE CHALLENGES TO THE MODERN INVESTIGATOR

Dan Blackman
Edith Cowan University, Security Research Institute
d.blackman0@our.ecu.edu.au

Abstract

Mobile Forensics has developed into an area of significant concern to law enforcement agencies and their counterparts, specifically as a result of individuals moving away from using traditional computers and focusing attention on their mobile device. Due to the smart phone being almost permanently attached to the person or in near proximity, it has become a significant source of information for investigators and can mean the difference between proving guilt or innocence. Tools have long been established, which provide agencies the ability to encapsulate expertise, which allows the easy download and production of reports for the mobile device and how it was used. However, whilst these tools work for the majority of devices in near perfect working condition they fail in cases where the phone is even slightly damaged. Many of the tools also require the investigator to unlock the phone or enable a feature before it can be downloaded. Should part of the phone be malfunctioning or if it prevents a feature or unlock from occurring, the ability to obtain forensic evidence will be reduced. Whilst devices can be surprisingly resilient at times, damage by throwing the device into a fire or snapping the logic board in half, will ultimately cause the device to be inoperable and beyond repair. The question therefore arises: How can the investigator even identify the model of device, considering parts of the device, including identification stickers, may have melted off or be missing? In such scenarios repairing the phone via changing the majority of the hardware from 'donor' phone cannot be conducted, as they are beyond repair. There is also no chance of being able to re-join the parts of a double or triple layer logic board and a re-joining a single layer logic board is both time and labour intensive. Even then there is no guarantee the phone will work again. To address these difficulties, significant monetary value needs to be invested in equipment and training to equip forensic investigators with the skills and ability in Chip-Off forensics and Ball Grid Array (BGA) rework.
These skills mean the small chips from the logic board can be removed without causing damage to their delicate legs or body, enabling the data they contain to be interpreted. Once interpreted, the investigator then has the ability to find what evidence was located on the device and hopefully leading to a conviction of guilt.

Keywords

Mobile Forensics, Chip-Off Forensics, BGA rework, Law Enforcement, JTAG

MOBILE FORENSICS AND LAW ENFORCEMENT

In June 2007, the number of mobile phone services exceeded the Australian population, with 21.26 million services connected. The ownership levels were their highest in age groups 18-34years and lowest in 65years+ (ACMA, 2009). In the June quarter of 2014 Australian's were found to have further abandoned their use of fixed line connections, further declining by 9.19 million, in line with previous years (ACMA 2014).

As a result, Australian's are using more data on their mobile devices than ever before. In June 2014 mobile phone users increased their downloads by 97.3% to over 38,734TB in a year. At the same time, there were a total of 12.07 million smart phone users in Australia, up 7.9% on the previous year. (ACMA, 2014).

Overall, Australian's are increasing their use and dependence of their mobile devices, year on year. However, as a result Police are finding more and more criminal activity as a consequence: More people are using their mobile phones to commit crimes against society. Even though individuals may not be committing crimes online, the simple knowledge that they will have their mobile device on their person provides Police with substantial evidence to place a person at a scene, at a particular time (Curran K., 2010).

Law enforcement is constantly challenged by individuals who do not wish to provide access credentials to their mobile devices, whether this be because of privacy concerns or to conceal information contained on their device that may provide some element of evidence or criminality (Jansen W., 2008). However ongoing advances in technology are assisting law enforcement.

Many more mobile devices can be downloaded now using commercial products than in the past and the list of mobile devices supported by these tools is ever expanding (UFED, 2015). The investigator, irrespective of the pin code, can also download some devices immediately. Some devices can have their pin lock overridden, whilst others can be downloaded if "USB Debugging" is enabled. In this instance, should it be required, the pattern lock or pin lock maybe downloaded and decoded from the gesture.key file located in the /data/system folder of the internal memory. However, unfortunately "USB debugging" is not enabled by default to prevent users from making unintended modifications to their mobile device (Lessard J., 2010).

Finally there have been times in the past where the supplier has co-operated with law enforcement for the purpose of unlocking a mobile device. Both Apple and Google required a US court subpoena and then would allocate a period of time for the investigator to attend and have their device unlocked. Such subpoena's in Australia needed to be applied for and vetted via the Attorney General's Mutual Legal Assistance Treaty (MLAT) (Brandis, 2014). However, recently Apple released version 9 of its iOS and Google released an update to the Android operating system, both of which do not allow the supplier to override the phone's passcode. This means both Apple and Google will be unable to unlock a phone, despite a court order (Timberg, 2014).

DAMAGED PHONES AND THEIR REPAIRABILITY

Many mobile devices require the forensic investigator to interact with the device to some degree. These interactions could be as simple as turning the phone on to using the touch display to enable a certain function, such as enabling USB debugging mode on the device.

However, depending on the extent of damage to the phone, some of these actions may not be possible. Clearly there are varying degrees of damage, which may allow the investigator to still obtain a full download of the mobile device.

In addition, every device requires some form of connection to be downloaded. Many of these connectors are particularly sensitive to foreign materials and are easily broken. Unless the mobile device has been recently purchased and then used to commit a crime, the modern forensic investigator needs to take into account wear and tear to the device, along with any damage, be it accidental or deliberate.

Focusing just on deliberate damage caused to a device, a number of examples are explored to help understand just how much damage can be inflicted on a mobile device before it can no longer be repaired and the data downloaded.

Surprisingly, as mobile devices become smaller and packed with more features, the difficulty in destroying them, with no means of recovery, becomes more and more acute. In addition, toughened glass, aluminium skins and protective casings make the task far more difficult without mechanical means.

Liquid damage

Figure 1: Water Damaged iPhone 4S

Whilst water damage can cause some significant damage to the electronics, particularly on shorting the battery terminals, if caught early enough the device can be usable again.

In the figure above, the phone was dropped into a glass of water for approximately two minutes. Both Litmus paper stickers, indicated by the arrows, changed from white to red indicating the presence of water inside. In the above photograph the water residue was also still present in the device a day after it had been exposed. Removal of the logic board found further water residue stuck underneath, between the logic board and the frame
assembly. It was found that the quickest and most effective way to remove this water residue was to completely disassemble the phone and dry the components individually. Leaving the phone in a sealed back with liquid absorbing desiccants for a weekend failed to remove large pools of liquid.

After drying completely, this device worked without any issues or damage to internal circuits, in fact it was found the battery still retained charge and was able to power the device.

However, the time a device spends immersed in liquid is a significant factor as to the amount of damage caused, particularly to the battery. Additionally phones immersed in moving liquids, such as rivers and washing machines can have serious damage to the logic board, LCD, and battery. This is due to the way water has the ability to can etch away slowly, similar to a cliff face. This in turn causes the tracks on the logic board to lift, lamination of the LCD to breakdown and a separation of the components within the phone.

The content of the liquid can also have a significant bearing on how quickly the device is damaged. The pH level along with the amount of salt contained in the liquid can determine how quickly the metals and plastics are broken down, along with how much corrosion builds up on the individual components (Klyatis, 2002), contacts and tracks of the logic board.

Typically on immersion, the battery will begin to increase in size and generate heat. The short circuit the water provides causes corrosion to form on battery terminals relatively quickly (Klyatis, 2002). Depending on where the liquid enters the phone first, further damage may also be caused to other components due to higher voltages where a lower voltage is required. Should this occur, replacement of the faulty components would be required.

Corrosion building on components is accelerated by a number of factors such as the temperature of the liquid, chemical pollutant, vibration in the liquid and any mechanical wear/removal of preventative films etc. (Klyatis, 2002)

Dragged / Friction damage

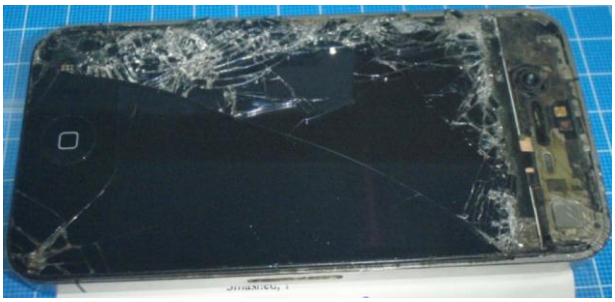

Figure 2: Friction damaged iPhone 4

Figure 3: Friction damaged iPhone 4

Kinetic Friction generally requires a device to be dragged along a hard surface, similar to a surface friction test. In the attached photos, significant damage can be seen to a device, which was thrown from a moving vehicle.

This device made contact with the road surface on a highway (100km/h limit) in Western Australia, bounced and then slid for an unknown distance. The top portion of the screen and digitizer were sheered away from the body of the phone and the rest of the screen. The round front facing camera, indicated by the arrow, is however still in its original position in the phone. The rubber mounting blocks attached to the front facing camera are missing, along with a number of the screw heads supporting the frame's integrity. Despite this, the phone did not loose structural integrity and remained intact.

Although there was the potential for significant damage, the logic board was not damaged and was protected by the frame of the phone (made of aluminium) and remaining LCD and digitizer components. The logic board was removed from this device and placed into a "donor phone", pin code bypassed and data successfully downloaded.

An unreadable mobile device due to kinetic friction is dependent on a number of factors. Firstly, the amount of time the device is subjected to an opposing friction force and therefore the amount of damage sustained by the device. Secondly, the state of the surface (coarseness, dirt, and other impurities) and the type of surface the mobile device is against. Thirdly, the force or pressure exerted of the surface to the mobile device and likewise the mobile device to the surface. Finally, the absence of any type of lubricant, preventing kinetic friction from forces causing damage to the mobile device (Fu H., 2011).

Whilst it maybe possible to subject a mobile device to laboratory tests, which cause it extensive damage, it is unlikely that the mobile device will find these tests replicated in real life. In fact in the example, the device sustained only minor damage compared to a test, which reduces the mobile device to grit.

Therefore the possibility a mobile device is completely unrepairable due to a friction is somewhat unlikely. Far more likely would be a damaged mobile device, due to the inertia experienced from contact made with the road surface.

Gun Shot and Impact damage

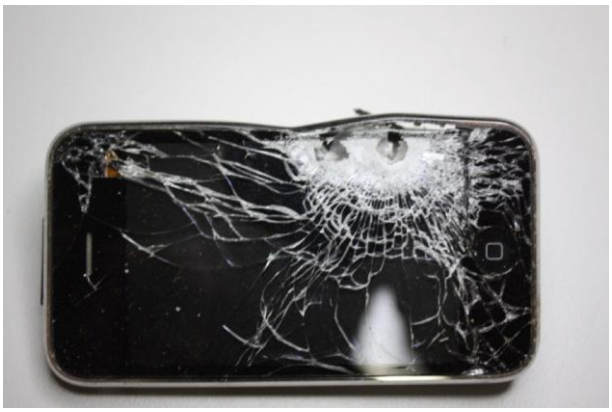

Figure 4: iPhone 3GS subjected to two rounds 6mm projectile

Figure 5: Single round through iPhone 4S

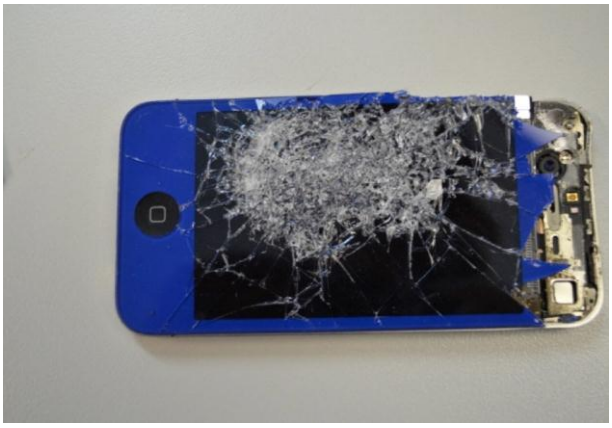

Figure 6: Impact weapon damaged iPhone 4

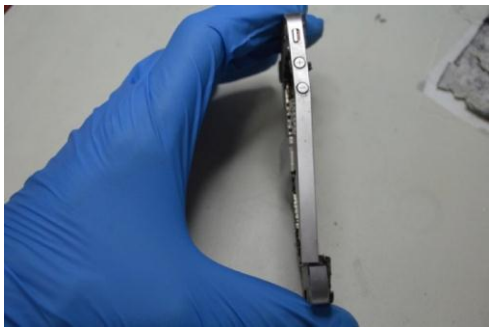

Figure 7: Shotgun loaded with "Bird shot" and damage caused on iPhone 4S frame

Many people would believe a gunshot to a mobile device would cause that device to never function again. However a number of factors are dependent on how fatal a gunshot can be to a mobile device.

Firstly, the mobile phone model, version and manufacturer can be important. The manufacturer, model and sometimes version will determine where the main logic board resides within the phone. Some mobile devices have a logic board, which consumes the entire length and width of the outer casing. Some devices store all of their data on a micro SD card inside the device, with very little on-board memory. Depending on the phone details, will directly affect how recoverable the data is from the device.

Secondly, there is much dependence placed on the location of any shots fired into the phone. Many Samsung Galaxy and Apple iPhones phones compact their logic boards and place them in the outer extremities of the mobile device so they can fill the inner portion of the phone with battery. The larger the battery can accommodate, the longer the mobile device can be used. Therefore in many cases a shot to the centre of the phone would only strike the battery, allowing (with some repairs) the phone to be completely downloaded, without any lost data. Likewise a shot be fired to the outer extremities of the device would have a greater chance of striking the logic board and solid-state storage, causing the data to be irrecoverable. This is contrary to much gun training, including for law enforcement, which train their officers to shoot at the centre seam of mass.

Thirdly, the type of ammunition and calibre can be important. A solid 12 gauge shot fired from a shut gun would have the ability to destroy much more of the phone compared to that of finer grained 'bird shot' pellets, fired from the same weapon. In the above figures, 'bird shot' was fired at an iPhone 4S. Although the screen and

frame were severely damaged, the aluminium casing behind the screen protected the logic board and subsequently the phone could be recovered. The same difference maybe found with to the design of the round; break apart on impact, or stay together. The comparison can find a significant difference in damage.

The same dependencies exist when considering the damage an impact weapon would inflict. The type and model of phone, locality of where the weapon strikes and the weapon itself can cause differing degrees of damage and recoverability of the device. Typically though, such as in the above figure, whilst an impact weapon appears to have destroyed the phone, in most cases the screen in merely broken and can be replaced.

Fire and Heat Damage

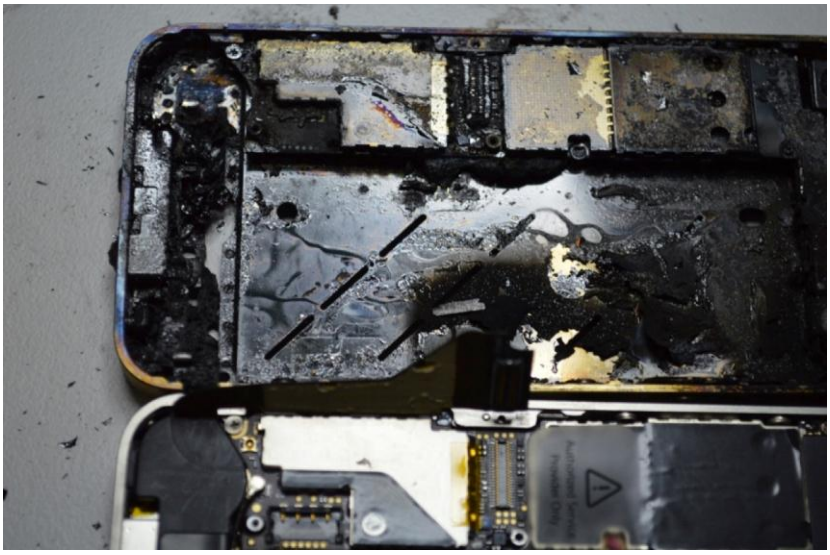

Figure 8: Heat damaged iPhone 4S (top) normal iPhone 4S bottom

Many electronic devices can tolerate a certain amount of heat before their components are compromised. To allow this many devices have heat reducing or heat dissipating foils/shields, similar to heat sinks in computers, which assist in preventing the microchips and circuit board from gathering too much heat.

The parts of a device with the lowest melting point and therefore the fastest to melt are the digitizer and liquid crystal display (LCD). Any other glass or plastics (such as the backing on many iPhones and connectors) will also melt quickly.

In the figure above, the device was subjected to a heat furnace for five minutes at approximately 300°C. This was enough time and heat to melt both the front and back glass and cause heat distress to portions of the aluminium frame. Additionally all plastic connectors were significantly damaged and portions of the iPhone tracks on the circuit board were damaged. This device has not been recovered at this time, as a result of the damage caused to the connectors and circuit board tracks. The only solution to recoverability is Chip-Off Forensics (discussed later), which may allow this device to be downloaded.

For devices damaged by heat and fire, recoverability of the device is dependent significantly on the amount of heat the device is subjected to, the length of time it is subjected to this heat source and how direct the heat source is on the device. In addition, the model of the phone can be a significant factor – if it has heat protective

measures incorporated and the makeup of metals and plastics in the device. As an example, a completely plastic Samsung galaxy may not sustain the same length of time subjected to heat to that of the aluminium covered iPhone 4S.

Joint Test Action Group (JTAG) & Pin locks

JTAG was formed to develop a method to test printed circuit boards after being manufactured. Mobile forensic technicians since discovered that the connection points used by these individuals also allows them to copy the data from the mobile devices in a forensically sound manner (Breeuwsma M., 2007). As a result of this the chips are accessed directly and no requirement for PIN numbers or unlock codes are required.

A successful JTAG download requires the investigator to carefully disassemble the mobile device and then to locate the JTAG points and identify what contact does what. As an example, the successful download of an HTC

EVO 4G mobile phone requires the forensic investigator to connect or solder to no less than eight solder pads on the motherboard.

In addition to the actual connection, a connection box is needed with specific software installed on it, to connect to the mobile device. This software is specific to the model of phone and in some cases, version of the firmware loaded on the mobile device. The JTAG box needs to be updated frequently and in some cases may not have suitable software for all versions of all mobile devices in the market.

A number of different JTAG boxes are available in the market, such as the Medusa box, RIFF box and ORT-JTAG box. Each has their own software interface, different connections and different lists of mobile devices they support. However the end goal is the same: To download a binary file, also known as a file dump, of the entire phone's on-board storage for forensic interrogation (Murphya C., 2015).

A pin lock bypass typically uses a type of brute force attack to unlock the device. The pin lock bypass device is usually an external device, which connects to the mobile phone and attempts to connect to the device. Some of these devices utilise vulnerabilities in the phone's operating system, whilst others attempt to simulate a keyboard when plugged into the phone. The result is every possible pin code combination attempted, unless the successful unlock code is found prior. A recent product called IP-BOX (Murphy, 2015) simulates a keyboard on the

iPhone. The device quickly restarts the mobile phone each time an unsuccessful code is found, to prevent unsuccessful attempts being recorded. The end result allows the device to attempt multiple passwords before the mobile phone locks all attempts completely. The biggest problem with this technique is the time taken: Approximately 111hours to exhaust the entire keyspace for a four-digit pin code. To reduce this time, other products make use of vulnerabilities (Ryan, 2014) in some versions of Apple's iOS to attempt multiple pin combinations. The use is required to interact with the mobile phone to enable these vulnerabilities. Once enabled the iPhone does not restrict the number of password attempts or the length of time between incorrect password attempts.

A major risk for any brute force attempt is the possibility data maybe modified on the mobile device and therefore the tampering with a forensic exhibit. A fundamental rule of computer forensics is to handle the exhibit as minimally as possible (Ryder, 2002). Unfortunately each brute force attempt on the original device maybe recorded on the device. Additionally, a risk exists if the device has an erase setting programmed to execute after

a series of unsuccessful pin attempts (typically ten). Unfortunately there is no distinct way to ascertain whether this software is configured or the number of unsuccessful attempts before the device erases. Therefore this attack method should be used with care so as to not erase the device and lose potential evidence on the device forever.

Chip-Off Forensics

For devices seriously damaged a simple repair will not restore their functionality. The only remaining solution is to conduct Chip-Off Forensic work. This work means the individual chips are removed from the circuit board and downloaded or attempts are made to reinstall them onto a working "donor" logic board.

Unfortunately this work is not without risks. Firstly, especially in the cases of fire, the chips are very fragile and the small pins (or legs) of the chip are extremely sensitive. Should the leg of a chip bend or fuse with another

leg, it maybe difficult to rectify. In the event a leg breaks off there is no way to reinstall it, and therefore the data is lost forever (Sansurooah, 2009).

In many cases controller chips and storage chips are stacked on top of each other. This stacking is typically used to reduce the size of the device and the size of the logic board required. For installation inside the factory, the chips are installed both at the same time by sophisticated automated machines. Unfortunately to remove these chips, the forensic investigator needs to de-solder each chip individually, carefully removing each and ensuring the chip below is not overheated in the process.

As devices are becoming smaller in size, but more functional, more components are required on the logic board of the devices. Many of the logic boards are responsible for all of the power requirements, connectivity to the various networks, storage of media, display and backlight along with large number of sensors. This all means that the forensic investigator is afforded a smaller area to work within, with typically multiple layer logic boards and varying component locations. To minimize space used, the chips themselves are smaller and require their legs to be space closed together, causing further difficulty to the forensic investigator.

Should they be successful in removing the microchips from the logic board, they then need to be cleaned and

‘re-balled’ or tinned with solder. This re-balling process requires each leg of the chip to have a small amount of solder re-applied to it to afford connectivity. Unfortunately too much solder may risk several legs being soldered together, whilst too little may give intermittent or unsatisfactory connectivity. In addition it has been found that reworking components multiple times may also cause them to diminish in reliability and degrade (Weidong X.,

2012).

Once connectivity issues are addressed, the investigator needs to attempt to download the data. Unfortunately this download and interpretation of data from the chip directly is typically time consuming (Swauger, 2014) and difficult based on multiple the multiple versions and models of microchips available.

An alternative solution is the possibility the microcontroller and the storage chip itself could be reinstalled on a new logic board with other working components. This technique also has risks and challenges, such as the alignment of the microchip and the how to re-solder of the chip to the logic board effectively. Little research in this area has been conducted, as it typically requires expensive machines and a level of automation for alignment reasons. Re-balling and rework techniques have long been developed for computer chips (Swauger, 2014), and there is no reason these techniques could not be applied to mobile devices.

Overall if the investigator can overcome these challenges, any damage caused to the logic board and connectors maybe overcome and a working exhibit could be presented to the court with data providing significant value to an investigation.

CONCLUSION

Mobile forensics is already a complex and difficult discipline without problems associated with damage to the device. Should the device be damaged by liquid, fire or friction, the amount of time the device is subjected, directly relates to the feasibility of recovery of that device.

Should gunshot, stabbing or slicing force damage the device, the location of that force on the device decides how easily the phone can be fixed and the data recovered. The location of the battery, logic board and other components can be in different locations in models of mobile phone. As a result two mobile devices, shot in the same location, can have very different outcomes.

In those cases where the device’s logic board is significantly damaged but the chips remain intact, the only possible technique remaining is Chip-Off forensics. However this technique is delicate in nature, potentially expensive and requires requiring precision equipment and training. This technique cannot be performed without dedicated professionals who have practice and procedures in place.

The techniques described in this paper are considered advanced and can consume vast amounts of the investigators time and resources. Therefore they maybe considered non economically viable for petty crimes. However where a mobile device is deliberately damaged, that device may contain significant evidence and lead to successful prosecution.

REFERENCES

ACMA. (2009). Communications Report 2008-2009. Retrieved October 20, 2015, from: http://www.acma.gov.au/webwr/_assets/main/lib311252/08-09_comms_report.pdf

ACMA. (2014). Communications report 2013–14. Retrieved October 20, 2015, from: http://www.acma.gov.au/~/media/Research%20and%20Analysis/Publication/Comms%20Report%202013%2014/PDF/Communications%20report%20201314_LOW-RES%20FOR%20WEB%20pdf.pdf

Brandis, G. (2014). Mutual Assistance Overview. Retrieved October 20, 2015, from: https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Documents/Mutual%20assistance%20overview.pdf

Breeuwsma M., J. M., Klaver C., Van Der Knijff R., Roeloffs M. (2007). Forensic Data Recovery from Flash Memory.

Curran K., R. A., Peacocke S., Cassidy S. (2010). Mobile Phone Forensic Analysis. *International Journal of Digital Crime and Forensics, 2*(2).

Fu H., F. L., Zhang G. (2011). Design and Manufacturing of Clutch in Tunnel Boring Machine. *Measuring Technology and Mechatronics Automation*.

Jansen W., D. A., Moenner L. (2008). Overcoming Impediments to Cell Phone Forensics. *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*.

Klyatis, L. M. (2002). Establishment of accelerated corrosion testing conditions. *Reliability and Maintainability Symposium, 2002. Proceedings. Annual*.

Lessard J., K. G. (2010). Android Forensics: Simplifying Cell Phone Examinations. *Digital Device Forensics Journal, 4*(1).

Murphy, C. (2015). IP Box Documentation-Rev2 01-16-2015.

Murphya C., L. A., Gaffneyc M., Punjad S. G. , Gibbe J. , McGarryf B. (2015). Windows Phone 8 Forensic Artifacts.

Ryan, S. (2014). CVE-2014-4451. Retrieved October 20, 2015, from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4451

Ryder, K. (2002). Computer Forensics – We've had an incident, who do we get to investigate?

Sansurooah, K. (2009). A forensics overview and analysis of USB flash memory devices. *7th Australian Digital Forensics Conference*.

Swauger, J. (2014). Chip-Off Forensics. Extracting a full bit-stream image from devices containing embedded flash memory.

Timberg, C. (2014). Apple devices to lock out police. *Washington Post*. Retrieved October 20, 2015, from: https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html

UFED. (2015). UFED Supported Devices. Retrieved October 20, 2015, from: http://lang.cellebrite.com/mobile-forensics/support/ufed-supported-devices

Weidong X., S. G. (2012). Effects of Multiple Reworks on the Accelerated Thermal Cycling and Shock Performance of Lead-Free BGA Assemblies. *IEEE Technology, 2*(11). doi: 10.1109/TCPMT.2012.2207722