Flasher Boxes: Back to Basics in Mobile Phone Forensics

Tue, 07/13/2010 - 10:46am by Digital Forensic Investigator

Every Contact Leaves a Trace

The mobile phone in today's society is without a doubt one of the most impressive revolutions of technology embraced by almost every person throughout the world regardless of race, color, or religion. Edmund Locard (1877-1966), a French criminologist, is regarded as a pioneer in the forensic world with his theory: "every contact leaves a trace," the Locard exchange principle. At the time he was inspired with this theory, I doubt very much he imagined that it would be as relevant in a modern technological world as it is today.

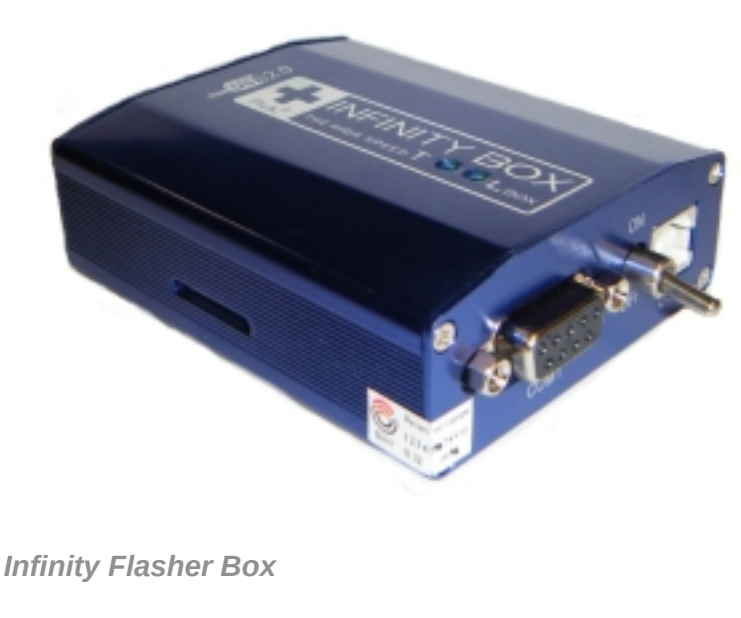
Simply switching on a mobile device—whether calls are made and received or not—will leave traces of data, not just on the handset but across a telecommunication network. Knowing where to look and understanding what can be retrieved to assist in a successful investigation is key to a case's swift and reliable conclusion. It is for this reason that the mobile phone has become an integral part of any modern day investigation.

Research by Dr. Jason Beckett in Australia has shown that evidence from cellular devices has increased by 500% in recent years. Is this because mobile phones were ignored and placed in the too difficult basket and are now being examined or that they are indeed being manipulated and used more extensively in the commission of criminal activity? Without a doubt the criminal fraternity is looking at mobile forensic manufacturers' websites and researching which devices are supported or not, as the case may be, prior to making their purchase. This has been evidenced numerous times in Mexico during investigations into organized crime involving the drug cartels.

So where do we go if big league criminals are taking such evasive action? "Back to Basics." There is a growing demand to return to the flasher box/hex dumping solution in order to retrieve information from suspect devices not supported by the various mobile forensic phone manufacturers. What are the alternatives? Thumb through the screen recording data as it appears? Certainly best practice would suggest that this be the first course of action regardless, when all else fails. Tools such as the Fernico ZRT and ZRT2 HD are excellent, easy to use products to facilitate this process. I use these tools on every single case regardless if it is a computer or mobile phone investigation to record a photographic survey of the device prior to and at the end of a forensic analysis. However, what about the latent data? What about damaged phones? What about phones without a SIM card? What about PIN protected handsets?

When Should You Use a Flasher Box

Let's be very clear before we go down the flasher box path, there is no replacement or substitute for the automated forensic tools produced by mobile forensic manufacturers such as: CelleBrite UFED or Physical Pro, Micro Sytemation XRY or XACT, Paraben Device Seizure Kit, Logicube CellDEK, or Susteen Secure-View to name but a few. Indeed these types of solutions should always be used as a first response. Unfortunately, with growing consumer demand for newer and more technologically advanced mobile phones, these automated and safe solutions do not meet some investigative requirements.



Infinity Flasher Box

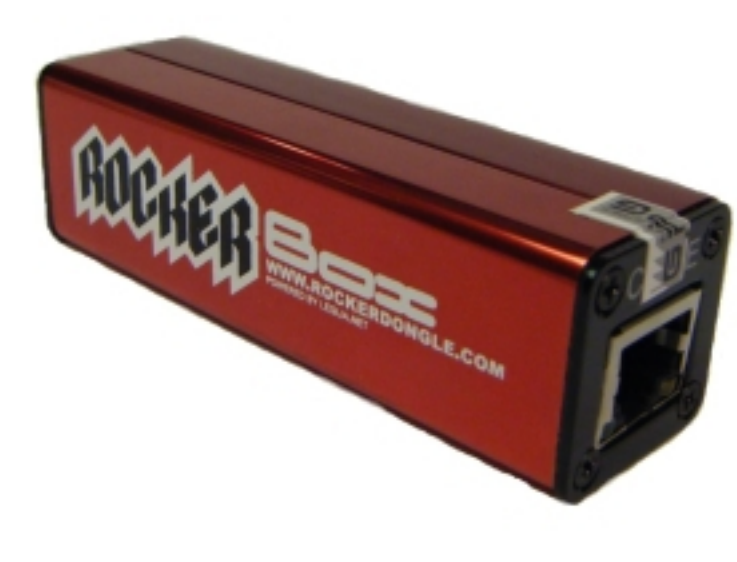
There is no question that flasher boxes are invasive alternatives, but this is where mobile phone forensics started prior to the commercially available fast copy, and more recently, forensic physical extraction tools. So is it safe to use them? Yes, by those who have been trained or have extensive experience in their use under controlled environments. What are the alternatives? Do you really want to leave evidence behind and just move on if the automated solution has failed you? If your conscience will allow you to leave potential evidence behind when a child predator has abducted a victim or a terrorist attack is imminent and you believe that using a flasher box is against the rules, then so be it.

Using all options available in a controlled and methodical manner to advance an investigation should be our desire. Don't stick your head in the sand like some eminent professionals and mobile forensic manufacturers, who advocate not using flasher boxes because they are not forensically sound. The trusted and well-established global protocols, such as the ACPO Guidelines for Computer-Based Electronic Evidence and the U.S. Department of Justice Electronic Crime Scene Investigations actually facilitate the use of such processes when all else fails, so who is to question them?

There were many sound convictions worldwide before EnCase and FTK came onto the computer forensic scene. Unfortunately, we are still at the pioneering stage in mobile phone technology and with the growth and complex structure of new devices appearing in the market place on a daily basis this will continue for some time. Those who purchase one automated forensic solution and think they can deal with every handset that comes through their laboratory are sadly mistaken. It is common to see multiple mobile forensic tools within a laboratory so why ignore or discredit any solution that can and does retrieve valuable evidence?

Flasher Boxes: Pros and Cons

All tools whether used for computer or mobile forensics must be validated and checked against each other. Prior to using any tool, investigators must consider the strengths and weaknesses of that tool and how to effectively apply it to the many different situations they will encounter. Flasher boxes do have weaknesses, amongst which are:



Rocker Flasher Box

- Flasher boxes are invasive.
- Changes to the data may occur.
- Some flasher boxes are technically challenging and complicated to use.
- Some do not create an audit trail or processing log.
- They do not perform hash verifications.
- There are many different boxes for the array of devices in the market place.
- Each flasher box can come with many different software interfaces.
- Proprietary and commercially sensitive information is often required for the correct interpretation of the extracted data.
- Analyzing the recovered data can be time consuming.

Given these weaknesses, why should flasher boxes be considered at all?

- A complete and reliable understanding of all activity is possible through the extraction and analysis of a hex dump taken from a suspect device.
- Truly deleted data from the handset can be retrieved.
- Damaged devices can be forensically examined.
- Data from devices where the SIM card is missing, damaged, or PIN protected can be recovered.
- Devices without a battery can be forensically examined.
- Data from PIN and other protected areas of a handset can be accessed.
- Analyzing the extracted data with automated processes is possible with such tools as: GetData Phone Image Carver, TagView, Hexaminer, CellPhone Analyzer, EnCase, and FTK using EnScripts and regular expression search terms.
- Utilizing the mobile forensic analysis software provided by CelleBrite Physical Pro and MicroSystemation, XRY Physical may also provide quality evidence when they cannot achieve an extraction of the raw data.
- Flasher boxes are alternative, cost effective solutions that provide truly deleted recovery capability for organizations on limited budgets.

Standard Operating Procedures

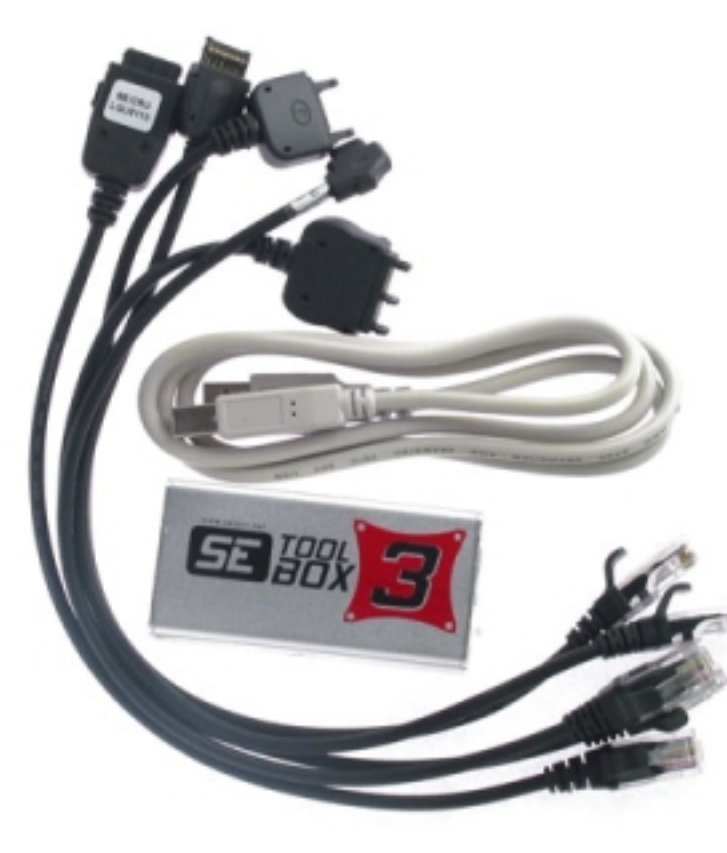
Using a combination of technologies, methodologies, and available tools has always been the most successful and productive way to investigate electronic media. It is therefore important to ensure the integrity and continuity of the extraction using tried and tested procedures and protocols.

The following are some basic guidelines that need to be considered to preserve the integrity of data when using a flasher box to extract it.

- Normal chain of custody documentation, as required by geographical jurisdiction.
- If the device is switched on, consider isolating it from a live network during its transportation and subsequent analysis.
  - Useful hints for temporary faraday solutions in an emergency:
    - Transportation – Using aluminum foil is an easy and quick way to isolate the device from communicating to a network. However, some foil is thin therefore it is recommended that the device be wrapped a minimum of five times to ensure it does not leak. Alternatively switch on the "flight mode" of the device to prevent it from communicating to the network if this option is supported on the suspect device.
    - Analysis – Most cities have underground parking lots. Identify a parking lot located below ground where no signal can be received. If the mobile forensic solution of choice has its own power supply or a portable power supply is available such as a cigarette lighter in most vehicles, the extraction can then be conducted with some degree of confidence. Some extractions can take some time, in which case underground lots are not a suitable option. Using the Ramsey Faraday portable solution may be an alternative, cost effective solution. Some devices boot to a "local mode," and therefore do not communicate to a network and their memory can be extracted without the use of a faraday environment.
  - Any solution chosen must be tested prior to using it on a live suspect device. The signal strength between service providers may vary, and there are many different makes and models of handsets available. Therefore, just because an LG XXX model on a Verizon network may not receive a signal five levels below the ground, do not take it for granted that a new iPhone 4G device on an AT&T network will not have the ability to communicate. Where possible test like for like, apples with apples, etc.
- Conduct a photographic survey of the device prior to commencing any extraction or analysis. Ensure that a record of any on screen activity is included, e.g. date and time stamps. This process is no different than handling a computer, as a picture tells a thousand words. Always use a trusted control date and time for the comparison of dates and times recorded on a suspect device. A recognized and acceptable method for such comparisons is the use of a GPS atomic clock.
- Where possible, ALWAYS use an appropriate mobile forensic extraction/copy tool to collect all available data prior to attempting to recover physical memory using a flasher box.
- If the flasher box creates an audit/processing log, this must be preserved and saved with the extracted hex dumped file. Consider recording the entire extraction via video if the selected flasher box does not record an audit log. This may not be practical as some extractions can be time consuming.
- DO NOT OPEN OR REVIEW THE EXTRACTED FILE ONCE IT HAS COMPLETED THE RECOVERY PROCESS.
- Create a forensic copy of the extracted data using FTK Imager or a similar tool that not only creates a secure forensic, read only copy of the extracted data but also generates a verification hash value of the extracted data. This phase should be done as soon as possible after the extraction to ensure the integrity and continuity of the evidence extracted.
- Conduct the analysis using the various forensic or HEX analysis tools of choice.

Conclusion

Do not put your head in the sand and have the death of a child or hundreds of people on your conscience because you ignored a possible alternative to interrogate a mobile phone when all else failed. Remember one thing "every contact leaves a trace". It's just a matter of where to look, how to retrieve it with integrity and controlled procedures, and what to use in retrieving it that makes the difference.



SE Tool Box 3 Flasher Box

References

ACPO Guidelines for Computer-Based Electronic Evidence

http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

U.S. Department of Justice Electronic Crime Scene Investigations
http://www.crime-scene-investigator.net/electronicCSIfirstresponder.pdf

Electronic Crime Scene Investigation: A Guide for First Responders
http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders
http://www.ncjrs.gov/pdffiles1/nij/227050.pdf

John (Zeke) Thackray *is the principal forensic investigator of Thackray Forensics Limited. Thackray Forensics an internationally recognized company that provides expert computer and mobile phone forensic services and training throughout the world. He can be reached at zeke@4n6.co.nz.*