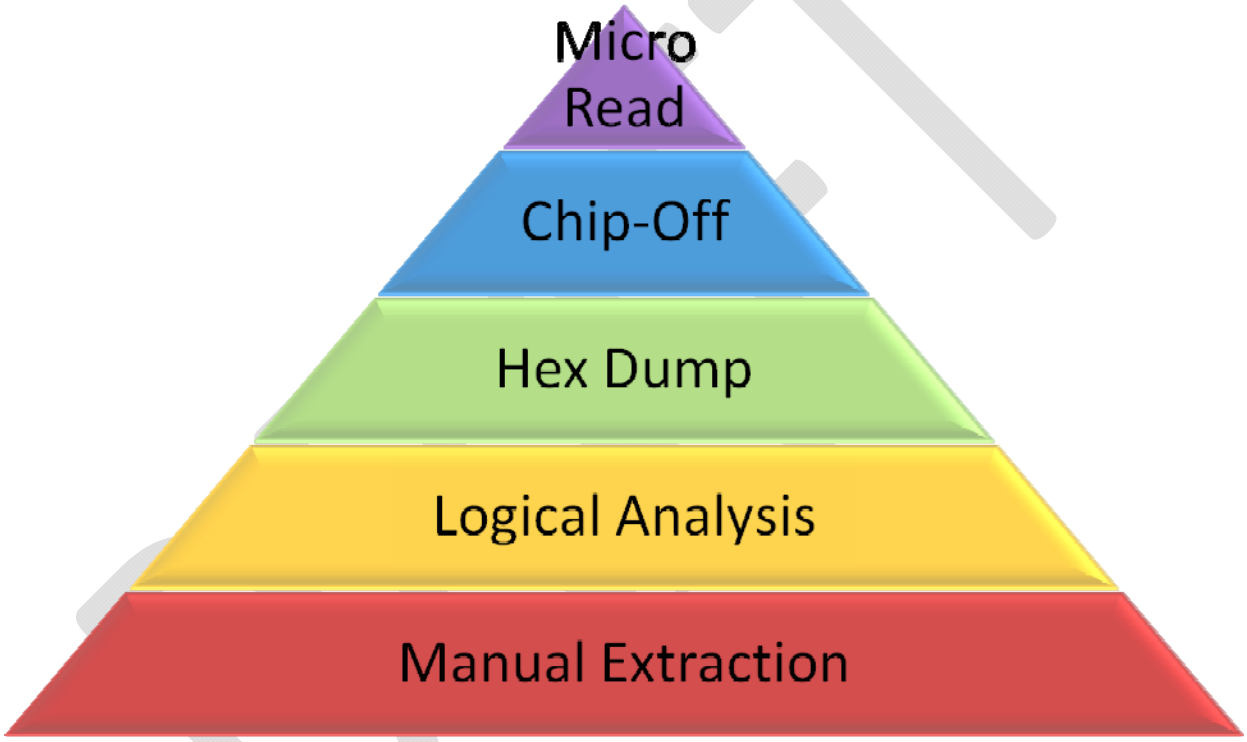
# iPhone Tool Classification

I have been processing a lot of iPhone's lately, and would like to share with you how many of the iPhone Forensic/Analysis tools fit into my Cell Phone/GPS tool classification system that I came up with several years ago. For those of you not yet familiar with the levels, I'll review them and then dive right into classifying the tools that are currently available. If you are interested, please contact me directly via email (sam@sambrothers.com) and I'll be happy to share a copy of my latest presentation for the classification of all Cell Phone/GPS tools as this is merely a sub-set of my original system.






Basically, the levels are a system by which any Cell Phone or GPS forensic/analysis tools can be categorized into. As you move UP the pyramid (generally):

- Methods get more "forensically sound"
- Tools get more expensive
- Methods get more technical
- Longer Analysis times
- More training required
- More invasive

**Level 1 (Manual Extraction):** This is where you review the phone documentation and then browse through the data using the buttons to view and record the information by hand from what shows up on the screen (LCD) of the device. This is also known as "hand jamming a phone". Problems with analysis at this level arise when the phone is physically damaged (e.g. Screen has been destroyed/removed or buttons fail to operate).

### *Tools for the iPhone/iTouch/iPad that operate at Level 1 include:*

1. **ZRT (**http://www.fernico.com/**)**
2. **Project-A-Phone (**http://www.projectaphone.com/**)**

**Level 2 (Logical Extraction):** At this level, a connection is established between the device (e.g. data cable, Bluetooth, or IR) and an analysis computer interface (e.g. USB or Serial). Communication between the phone and the computer is established using a variety of protocols (BREW, AT Commands, F-BUS etc.). Communication works in a client/server type architecture in the following manor:

1. A command is initiated by the computer and sent to the phone via the established connection.
2. The command is then processed and interpreted by the processor in the phone
3. The requested data is retrieved
4. The resultant data is communicated back across the communication conduit to the computer.

This Logical level type of analysis suffers from many issues. One such example is when the data port is disabled altogether such as in some disposable phones (e.g. many Motorola TracFone's).

*Note: Many of the tools listed below are able to also parse and present data stored on a computer from an iTunes backup. Also, I did not include tools that only parse/present iTunes backup file data. While good information can gleaned from an iTunes backup (if available), this paper does attempt not take into consideration the parsing of this iTunes data.*

### *Tools for the iPhone/iTouch/iPad that operate at Level 2 include:*

1. **UFED Standard (**http://www.cellebrite.com**)**
2. **XRY (**http://www.msab.com**)**
3. **Mobilyze (**http://www.blackbagtech.com**)**
4. **SecureView$^2$ (**http://mobileforensics.susteen.com**)**
5. **MobilEdit! (**http://www.mobiledit.com**)**
6. **Oxygen Forensic (**http://www.oxygen-forensic.com**)**
7. **Wolf (Sixth Legion)**
8. **CellDEK (**http://www.logicube.com**)**
9. **iPhone Extractor (**http://agapeforensic.com**)**
10. **Mobile Phone Examiner (**http://www.accessdata.com**)**

11. **Lantern (**http://katanaforensics.com**)**
12. **Aceso (**http://www.radio-tactics.com**)**
13. **Athena (**http://www.radio-tactics.com**)**
14. **Device Seizure (**http://www.paraben.com**)**
15. **Neutrino (**www.guidancesoftware.com**)**

**Level 3 (Physical Extraction):** Now we get to **some** of the fun stuff! This is where "Hex Dumping" comes in. At this level a connection is established as in Level 2, however, a boot loader or unsigned code is pushed into the memory of the phone and all (or almost all) of the data stored on the phone is pushed across the communication conduit and stored on the computer in a raw HEX (binary) format (hence the name "Hex Dumping"). "Analysis of raw hex data is time consuming and quite challenging which is a barrier for many examiners Over the last 2-3 years, many vendors have begun to support more and more phones at this level. This level also includes connecting to the diagnostic (e.g. J-TAG) connections on the phone to obtain data.

### *Tools for the iPhone/iTouch/iPad that operate at Level 3 include:*

1. **The Zdziarski Method (**http://www.iphoneinsecurity.com**)**
2. **iXAM (**http://www.ixam-forensics.com**)**
3. **XACT (**http://www.msab.com**)**

**Level 4 (Chip-Off):** This is where the memory chip (e.g. NAND Flash) is physically removed from the device, the chip is placed in an chip reader and all of the data stored on the chip is read and stored on a computer. This method is most like modern computer hard disk forensics analysis. While this may seem like a VERY forensically sound method, significant challenges exist here as well. They include but are not limited to: long times to interpret the raw data, non-contiguous data storage, a myriad of chip types and device damage during chip extraction. It should be noted that some devices store data (at rest) in an encrypted format (e.g. iPhone 3Gs), so this would require recover of the encryption keys as well to decrypt the data.

### *Tools for the iPhone/iTouch/iPad that operate at Level 4 include:*

1. **FlashDoctor (**http://www.salvationdata.com/**)**

**Level 5 (Micro Read):** Now we reach the coup de grâce! This is where the bits are read manually (or OCR'd). This requires manual interpretation of the status of the physical gates (e.g. Open, Closed, Open, Open, Closed, Open, Open, Open which may translate to: 010010000 which then translates to the ASCII letter: "H". Several layers of this type of translation make this level of analysis very time consuming and expensive. This type of analysis is ideal when a chip has been physically damaged.

### *Tools for the iPhone/iTouch/iPad that operate at Level 5 include:*

1. **No commercially available tools at this time.**

## *Closing:*

If I have missed listing a tool here, please let me know! If you send me an email, I'd be happy to consider your feedback!

I think that in the future, we will continue to see more and more tools move into Level 3 over the next few years. I anxiously await the opportunity to review the first Level 4 commercial tool!

## *Thank You:*


- Ryan Kubasiak – For pushing me to finally write this. If you like it, thank him! If you hate this, it's his fault!
- Jonathan Zdziarski – For infecting me with your undying search for knowledge.
- Andrew Hoog – For your methodological and logical approach.
- Rick Mislan – For helping me start on this journey to begin with.
- Rick Ayers – For being a good friend and a good sounding board for my ideas.