NIST Mobile Forensics Workshop and Webcast

Mobile Device Forensics:

A – Z

Homeland Security

June 2014

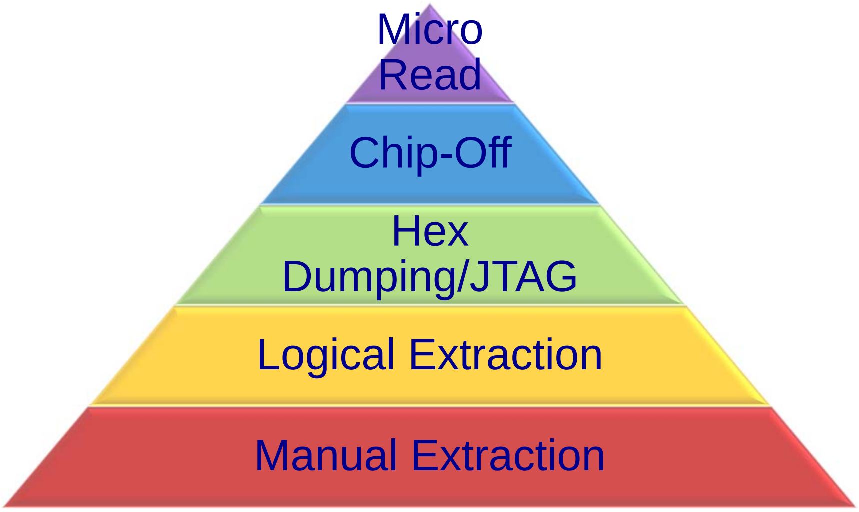
Disclaimer:

Certain commercial entities, equipment, or materials may be identified in this presentation. Such identification is not intended to imply recommendation nor endorsement by myself nor my employer, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

I have NO financial nor commercial interest in any of the products I will be discussing today!

U.S. Customs and Border Protection

Mobile Forensic Tool Classification



Micro Read

Chip-Off

Hex Dumping/JTAG

Logical Extraction

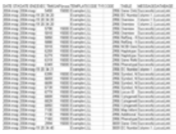
Manual Extraction

U.S. Customs and
Border Protection

How Mobile Forensic Tools Actually Work…

1. The broken tool story…

2. Proposed Changes…



3. Tool Leveling System

U.S. Customs and
Border Protection

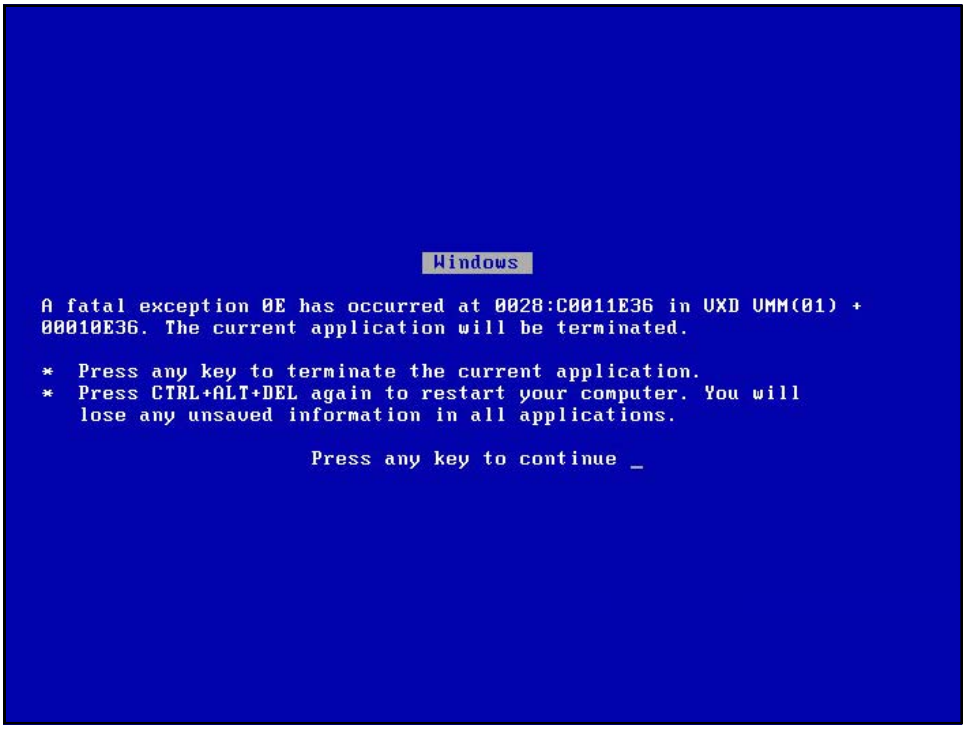
But first, the broken tool story…

U.S. Customs and
Border Protection

The broken tool story…

- Purchased tool “X” from company Y.
  - 8PM on Saturday evening… I hit the “get data button” and then…

U.S. Customs and
Border Protection



```
                              Windows

A fatal exception 0E has occurred at 0028:C0011E36 in VXD VMM(01) +
00010E36. The current application will be terminated.

*  Press any key to terminate the current application.
*  Press CTRL+ALT+DEL again to restart your computer. You will
   lose any unsaved information in all applications.

                      Press any key to continue _
```

Options:

A. Email encrypted debug logs to company Y support for analysis

B. Try different combinations till it works

C. Try another tool

D. Quit and become a pro card counter

E. Figure out why the tool is broken myself!

U.S. Customs and
Border Protection

And I…

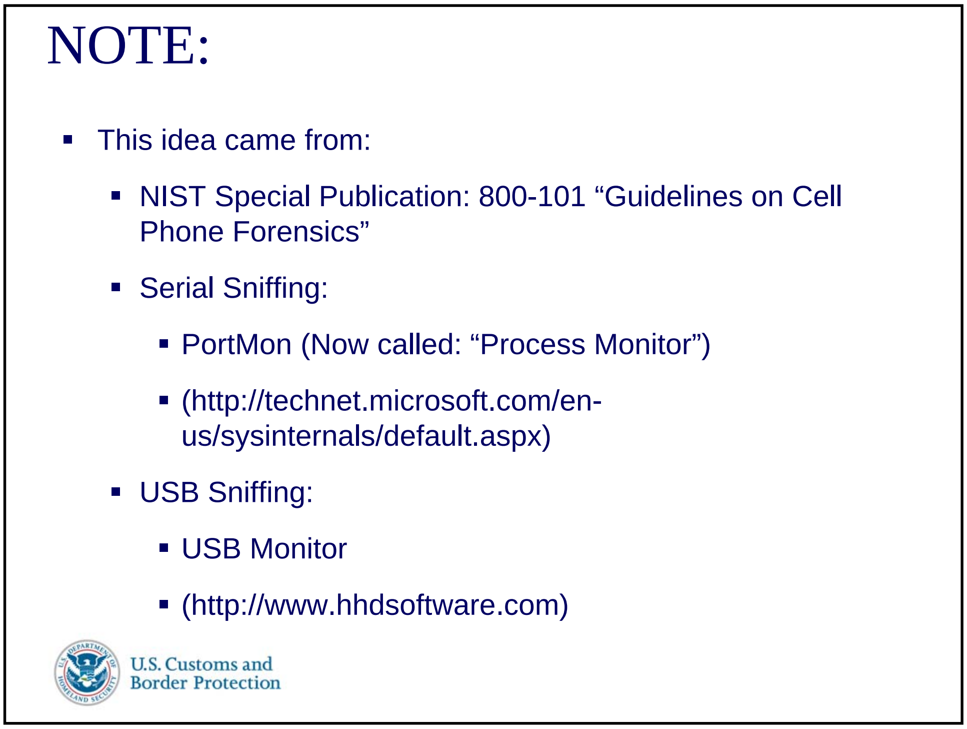
- I took the road less traveled…

U.S. Customs and Border Protection

A methodical approach:

- Wearing my "Malware Analysis" hat…
- I read* that running PortMon for Windows would allow a "diagnostic view" of the data.
- Voila!

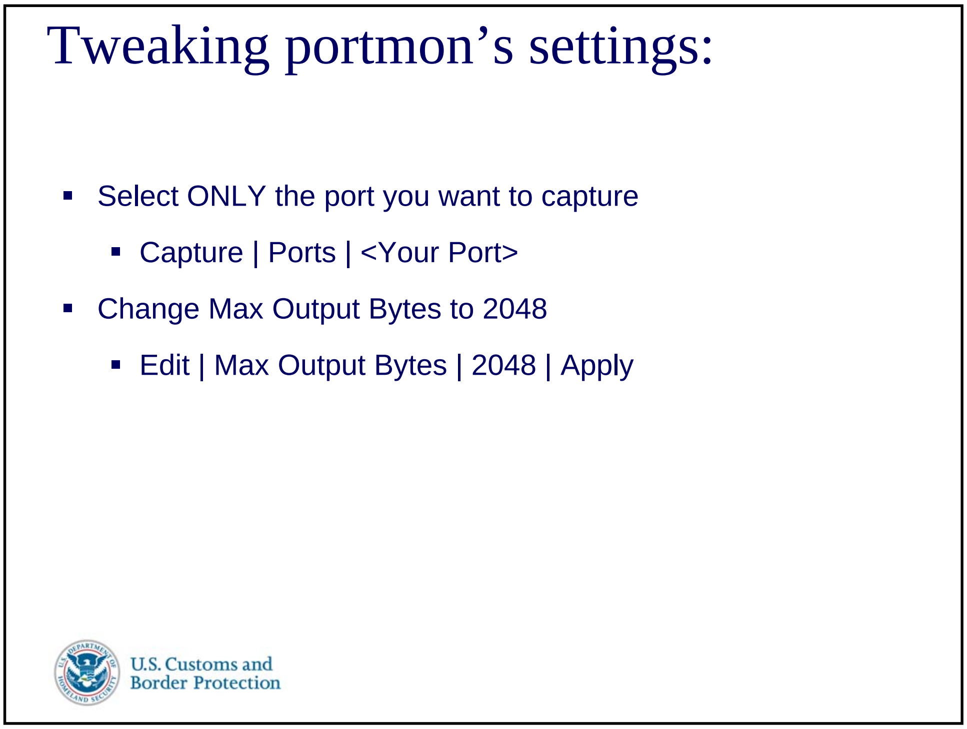
U.S. Customs and Border Protection



NOTE:

- This idea came from:
  - NIST Special Publication: 800-101 “Guidelines on Cell Phone Forensics”
  - Serial Sniffing:
    - PortMon (Now called: “Process Monitor”)
    - (http://technet.microsoft.com/en-us/sysinternals/default.aspx)
  - USB Sniffing:
    - USB Monitor
    - (http://www.hhdsoftware.com)

U.S. Customs and Border Protection



Tweaking portmon’s settings:

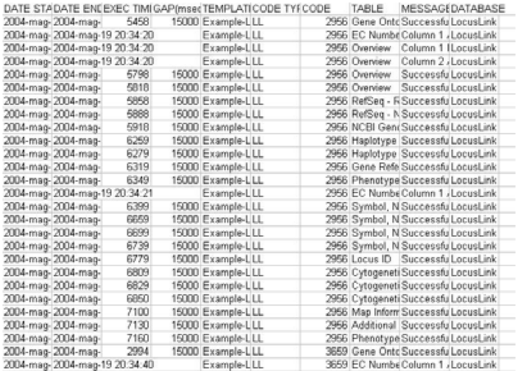
- Select ONLY the port you want to capture
  - Capture | Ports | <Your Port>
- Change Max Output Bytes to 2048
  - Edit | Max Output Bytes | 2048 | Apply

U.S. Customs and Border Protection

Things that make you go hmm…..

- You can use this to:
  - Compare different tools
  - How protocols work.
  - Application error checking.
  - See what data is NOT reported to you by the tool.
  - Observe the tool communication in real time.

Lots of options…



DATE STA	DATE END	EXEC TIMI	GAP(msec	TEMPLATI	CODE TYI	CODE	TABLE	MESSAGE	DATABASE
2004-mag-	2004-mag-	5458	15000	Example-L	LL	2956	Gene Ontc	Successfu	LocusLink
2004-mag-	2004-mag-19 20:34:20			Example-L	LL	2956	EC Numbe	Column 1 ,	LocusLink
2004-mag-	2004-mag-19 20:34:20			Example-L	LL	2956	Overview	Column 1 I	LocusLink
2004-mag-	2004-mag-19 20:34:20			Example-L	LL	2956	Overview	Column 2 ,	LocusLink
2004-mag-	2004-mag-	5798	15000	Example-L	LL	2956	Overview	Successfu	LocusLink
2004-mag-	2004-mag-	5818	15000	Example-L	LL	2956	Overview	Successfu	LocusLink
2004-mag-	2004-mag-	5858	15000	Example-L	LL	2956	RefSeq - R	Successfu	LocusLink
2004-mag-	2004-mag-	5888	15000	Example-L	LL	2956	RefSeq - N	Successfu	LocusLink
2004-mag-	2004-mag-	5918	15000	Example-L	LL	2956	NCBI Gen(	Successfu	LocusLink
2004-mag-	2004-mag-	6259	15000	Example-L	LL	2956	Haplotype	Successfu	LocusLink
2004-mag-	2004-mag-	6279	15000	Example-L	LL	2956	Haplotype	Successfu	LocusLink
2004-mag-	2004-mag-	6319	15000	Example-L	LL	2956	Gene Refe	Successfu	LocusLink
2004-mag-	2004-mag-	6349	15000	Example-L	LL	2956	Phenotype	Successfu	LocusLink
2004-mag-	2004-mag-19 20:34:21			Example-L	LL	2956	EC Numbe	Column 1 ,	LocusLink
2004-mag-	2004-mag-	6399	15000	Example-L	LL	2956	Symbol, N	Successfu	LocusLink
2004-mag-	2004-mag-	6659	15000	Example-L	LL	2956	Symbol, N	Successfu	LocusLink
2004-mag-	2004-mag-	6699	15000	Example-L	LL	2956	Symbol, N	Successfu	LocusLink
2004-mag-	2004-mag-	6739	15000	Example-L	LL	2956	Symbol, N	Successfu	LocusLink
2004-mag-	2004-mag-	6779	15000	Example-L	LL	2956	Locus ID	Successfu	LocusLink
2004-mag-	2004-mag-	6809	15000	Example-L	LL	2956	Cytogeneti	Successfu	LocusLink
2004-mag-	2004-mag-	6829	15000	Example-L	LL	2956	Cytogeneti	Successfu	LocusLink
2004-mag-	2004-mag-	6850	15000	Example-L	LL	2956	Cytogeneti	Successfu	LocusLink
2004-mag-	2004-mag-	7100	15000	Example-L	LL	2956	Map Inform	Successfu	LocusLink
2004-mag-	2004-mag-	7130	15000	Example-L	LL	2956	Additional	Successfu	LocusLink
2004-mag-	2004-mag-	7160	15000	Example-L	LL	2956	Phenotype	Successfu	LocusLink
2004-mag-	2004-mag-	2994	15000	Example-L	LL	3659	Gene Ontc	Successfu	LocusLink
2004-mag-	2004-mag-19 20:34:40			Example-L	LL	3659	EC Numbe	Column 1 ,	LocusLink

Think about it…

- Many tools still use a Serial Port, you may use this method to log all I/O during data collection:

1. Tool validation
2. Error Checking
3. Legal Proceedings
4. Tool Comparison
5. Free
6. Other tools work nearly the same for direct USB communication (USBSnoop)

U.S. Customs and
Border Protection

What was next…

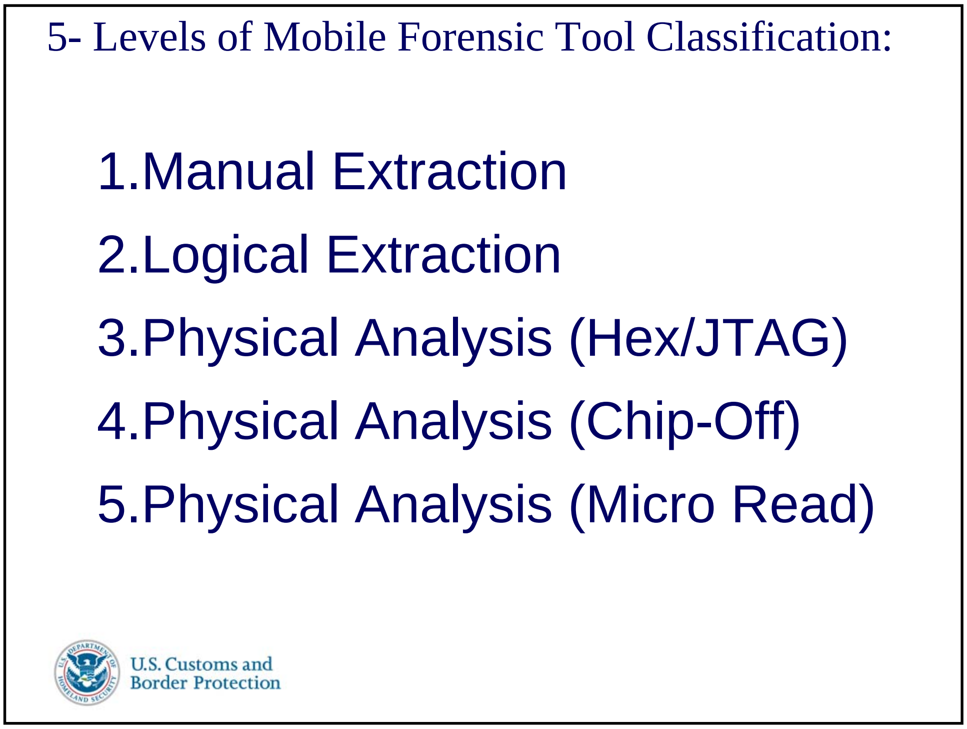
- In communicating this concept to fellow peers, it occurred to me…

U.S. Customs and
Border Protection

Mobile Forensic Tool Classification

- A common method/framework to describe HOW data is extracted from digital devices (e.g., Phones and GPS)
- Provides a common ground for all Mobile Examiners
- Vendors could classify tools

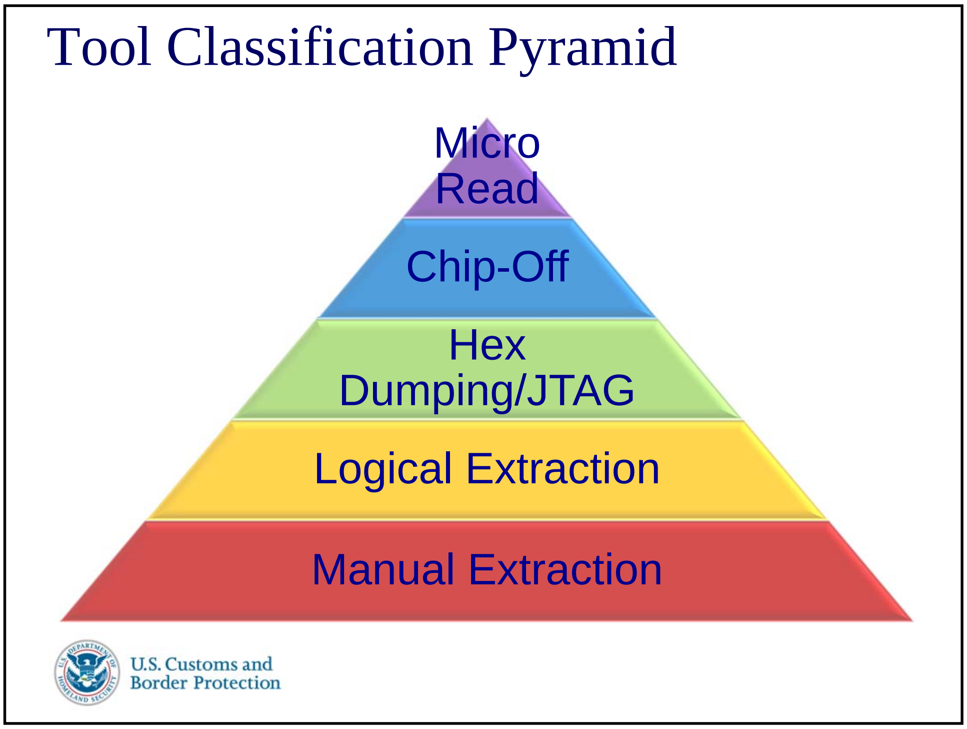
Mobile Forensic Tool Classification System…



5- Levels of Mobile Forensic Tool Classification:

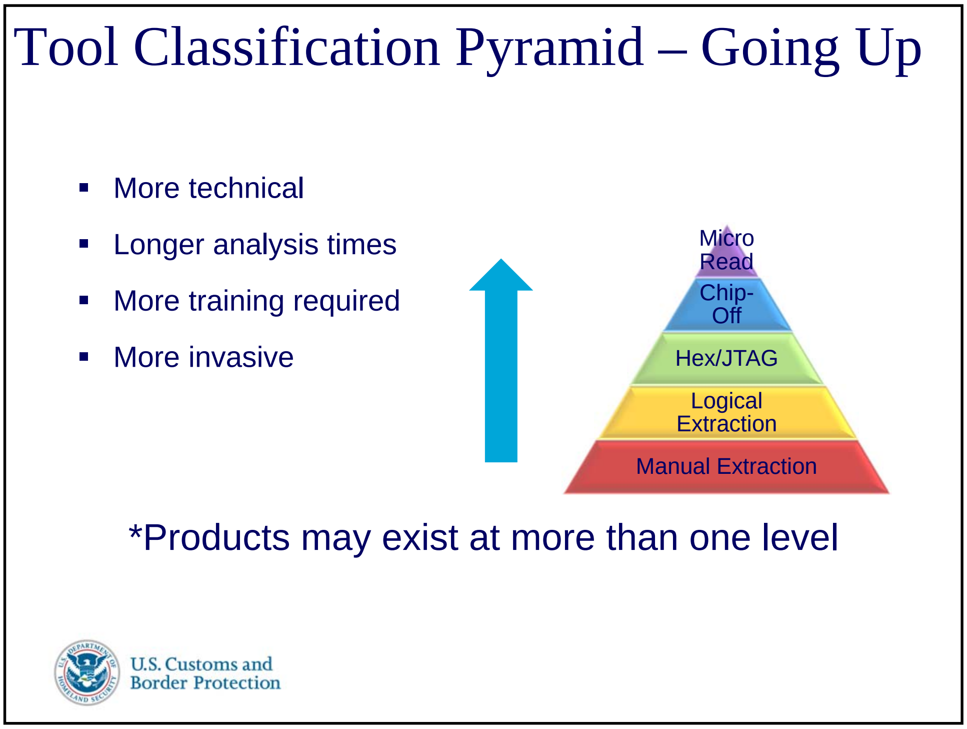
1. Manual Extraction
2. Logical Extraction
3. Physical Analysis (Hex/JTAG)
4. Physical Analysis (Chip-Off)
5. Physical Analysis (Micro Read)

U.S. Customs and Border Protection



Tool Classification Pyramid

U.S. Customs and Border Protection

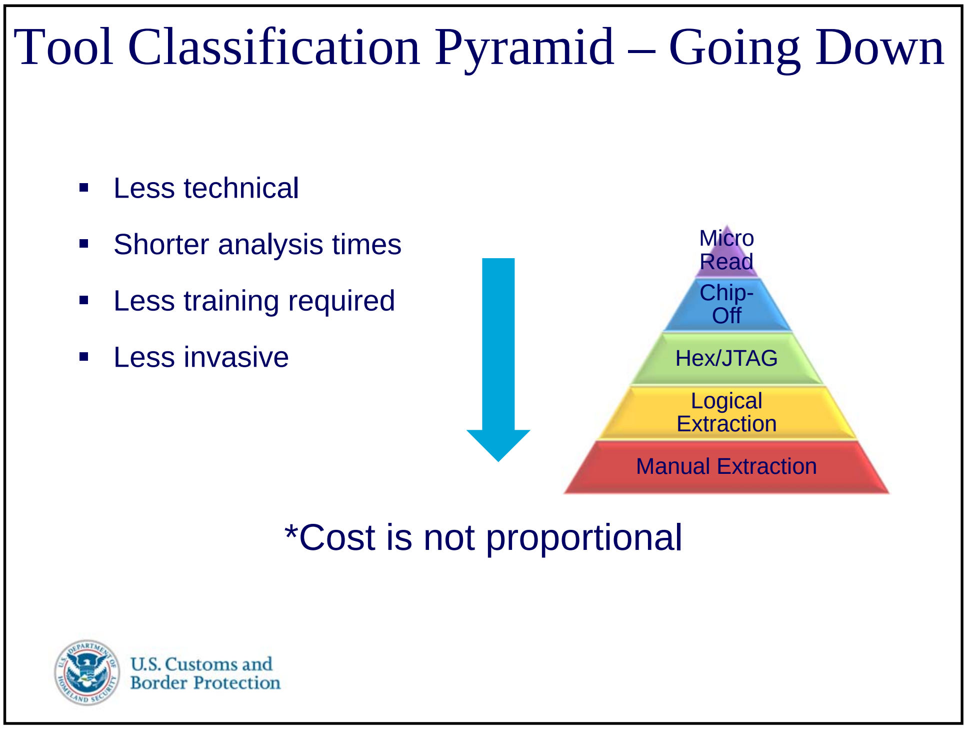


Tool Classification Pyramid – Going Up

- More technical
- Longer analysis times
- More training required
- More invasive

*Products may exist at more than one level

U.S. Customs and Border Protection

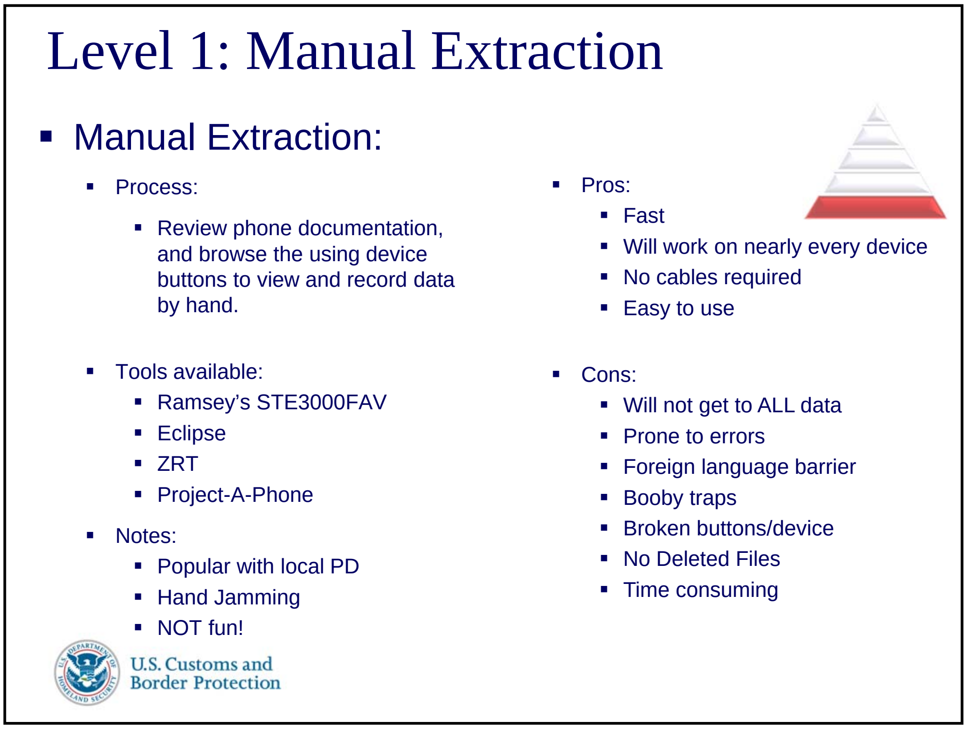


Tool Classification Pyramid – Going Down

- Less technical
- Shorter analysis times
- Less training required
- Less invasive

*Cost is not proportional

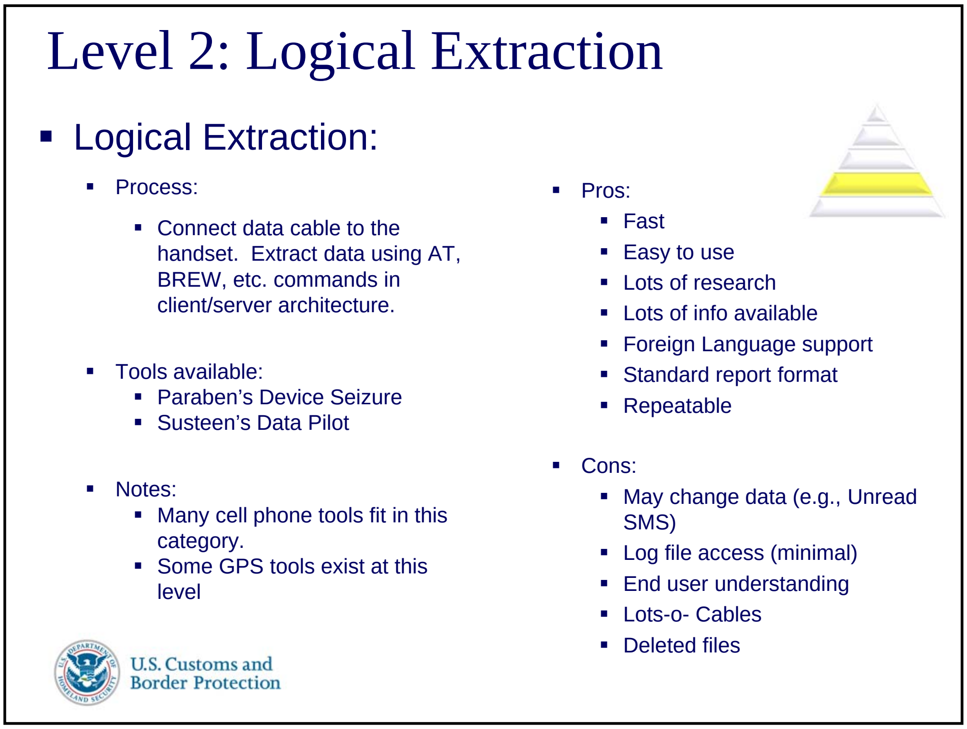
U.S. Customs and Border Protection



Level 1: Manual Extraction

- Manual Extraction:
  - Process:
    - Review phone documentation, and browse the using device buttons to view and record data by hand.
  - Tools available:
    - Ramsey's STE3000FAV
    - Eclipse
    - ZRT
    - Project-A-Phone
  - Notes:
    - Popular with local PD
    - Hand Jamming
    - NOT fun!
  - Pros:
    - Fast
    - Will work on nearly every device
    - No cables required
    - Easy to use
  - Cons:
    - Will not get to ALL data
    - Prone to errors
    - Foreign language barrier
    - Booby traps
    - Broken buttons/device
    - No Deleted Files
    - Time consuming

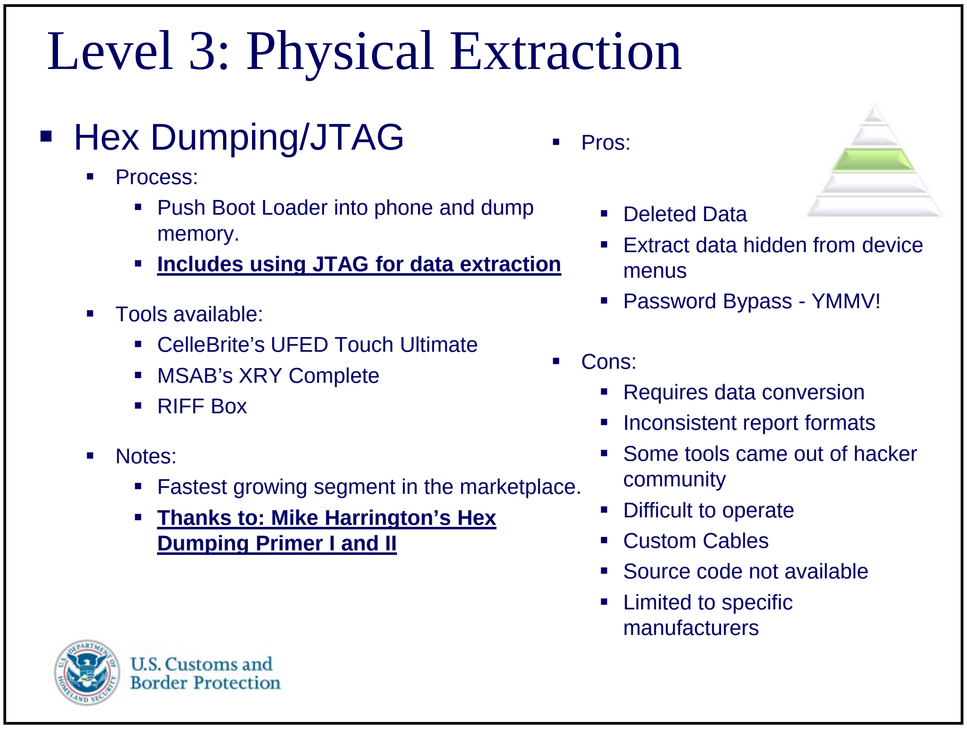
U.S. Customs and Border Protection



Level 2: Logical Extraction

- Logical Extraction:
  - Process:
    - Connect data cable to the handset. Extract data using AT, BREW, etc. commands in client/server architecture.
  - Tools available:
    - Paraben's Device Seizure
    - Susteen's Data Pilot
  - Notes:
    - Many cell phone tools fit in this category.
    - Some GPS tools exist at this level
  - Pros:
    - Fast
    - Easy to use
    - Lots of research
    - Lots of info available
    - Foreign Language support
    - Standard report format
    - Repeatable
  - Cons:
    - May change data (e.g., Unread SMS)
    - Log file access (minimal)
    - End user understanding
    - Lots-o- Cables
    - Deleted files

U.S. Customs and Border Protection

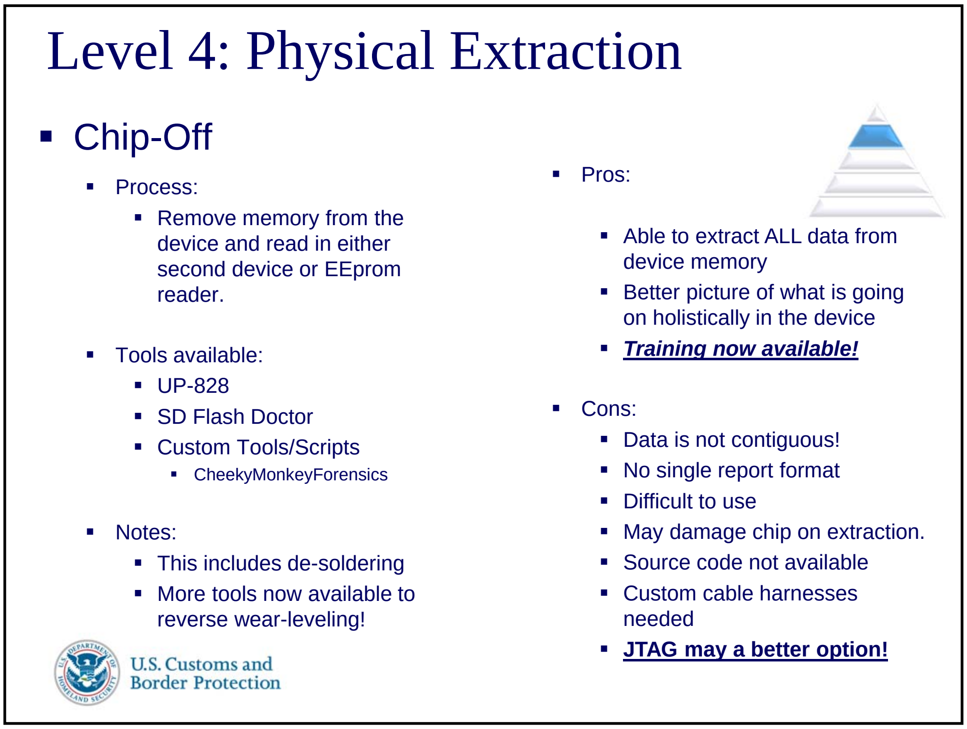


Level 3: Physical Extraction

- Hex Dumping/JTAG
  - Process:
    - Push Boot Loader into phone and dump memory.
    - **Includes using JTAG for data extraction**
  - Tools available:
    - CelleBrite's UFED Touch Ultimate
    - MSAB's XRY Complete
    - RIFF Box
  - Notes:
    - Fastest growing segment in the marketplace.
    - **Thanks to: Mike Harrington's Hex Dumping Primer I and II**

- Pros:
  - Deleted Data
  - Extract data hidden from device menus
  - Password Bypass - YMMV!
- Cons:
  - Requires data conversion
  - Inconsistent report formats
  - Some tools came out of hacker community
  - Difficult to operate
  - Custom Cables
  - Source code not available
  - Limited to specific manufacturers

U.S. Customs and Border Protection



Level 4: Physical Extraction

- Chip-Off
  - Process:
    - Remove memory from the device and read in either second device or EEprom reader.
  - Tools available:
    - UP-828
    - SD Flash Doctor
    - Custom Tools/Scripts
      - CheekyMonkeyForensics
  - Notes:
    - This includes de-soldering
    - More tools now available to reverse wear-leveling!

- Pros:
  - Able to extract ALL data from device memory
  - Better picture of what is going on holistically in the device
  - ***Training now available!***
- Cons:
  - Data is not contiguous!
  - No single report format
  - Difficult to use
  - May damage chip on extraction.
  - Source code not available
  - Custom cable harnesses needed
  - **JTAG may a better option!**

U.S. Customs and Border Protection

Level 5: Physical Extraction

- Micro Read
  - Process:
    - Use a high-power microscope to view state of memory.
  - Tools available:
    - High-Power Microscope
  - Notes:
    - This method would be reserved for high value devices or damaged memory chips.
  - Pros:
    - Able to extract and verify all data from device memory
    - Best picture of what is going on holistically in the device
  - Cons:
    - Most time consuming
    - Hard to interpret/convert
    - No report format
    - VERY Expensive
    - Highly technical

U.S. Customs and
Border Protection

Leveling System Examples:

- ZRT2 – **Level 1**
- Data Pilot – **Level 2**
- UFED Touch Ultimate – **Level 3**
- UP-828 – **Level 4**
- Hitachi S-450 SEM – **Level 5**

Level 1

Level 2

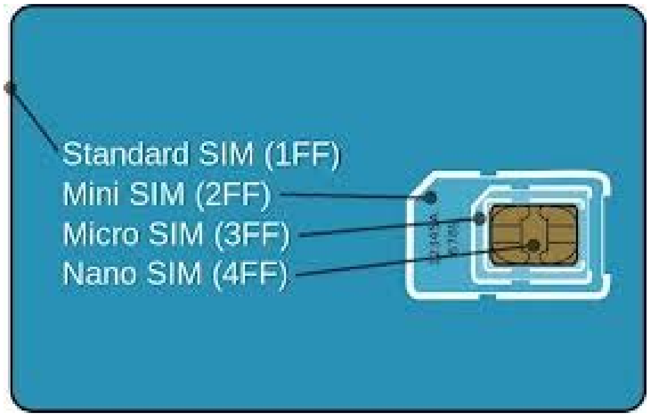
Level 3

Level 4

Level 5

U.S. Customs and
Border Protection

Standard, Mini, Micro & Nano…



U.S. Customs and
Border Protection

CSIM's/RUIM's

C-SIM = CDMA Subscriber Identity Module

✓For CDMA handsets to extend a GSM SIM card for CDMA phones and networks.

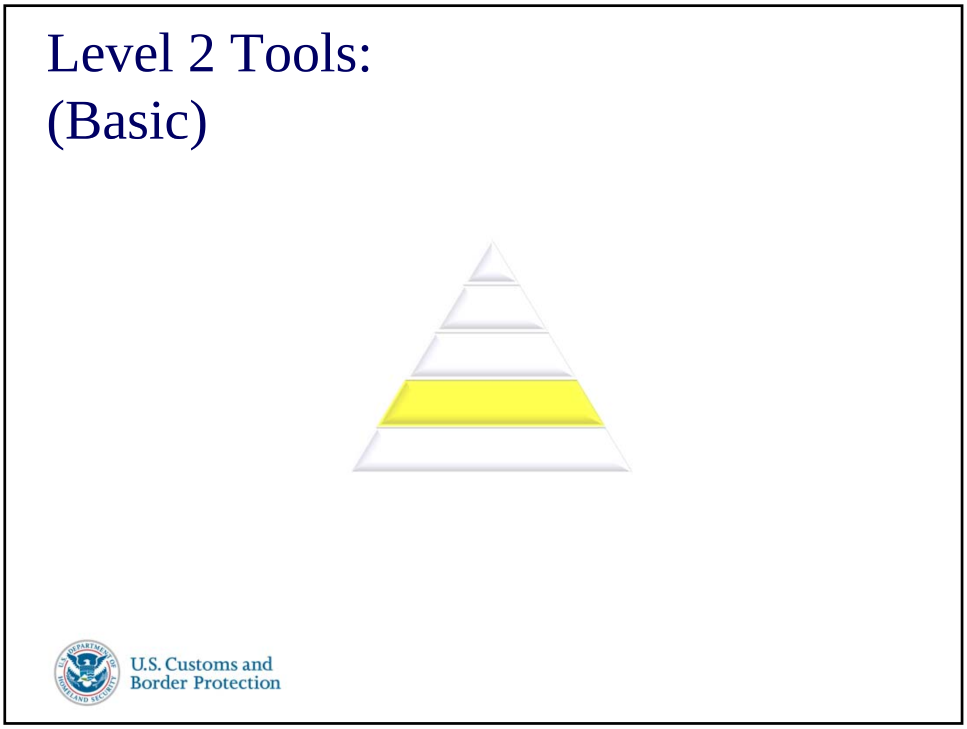
✓UICC may have: C-SIM, GSM **and** U-SIM partitions/application!

✓Only commercial tool I know of right now is: SIMIS (3g Forensics – Lester Wilson)

U.S. Customs and
Border Protection

Level 1 Tools:

U.S. Customs and
Border Protection



Level 2 Tools:
(Basic)

U.S. Customs and
Border Protection

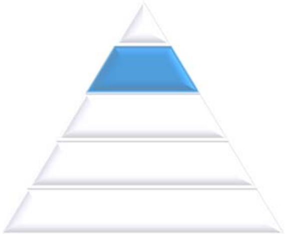
Level 2/3 Tools: (Basic)

U.S. Customs and
Border Protection

Level 3 Tools: (Advanced)

U.S. Customs and
Border Protection

Level 4 Tools:
(Chip Off)

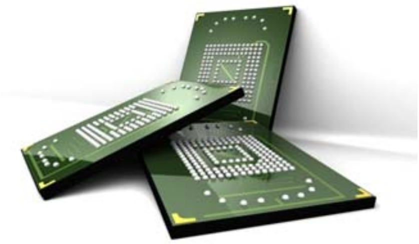


U.S. Customs and Border Protection

Pieces and Parts…

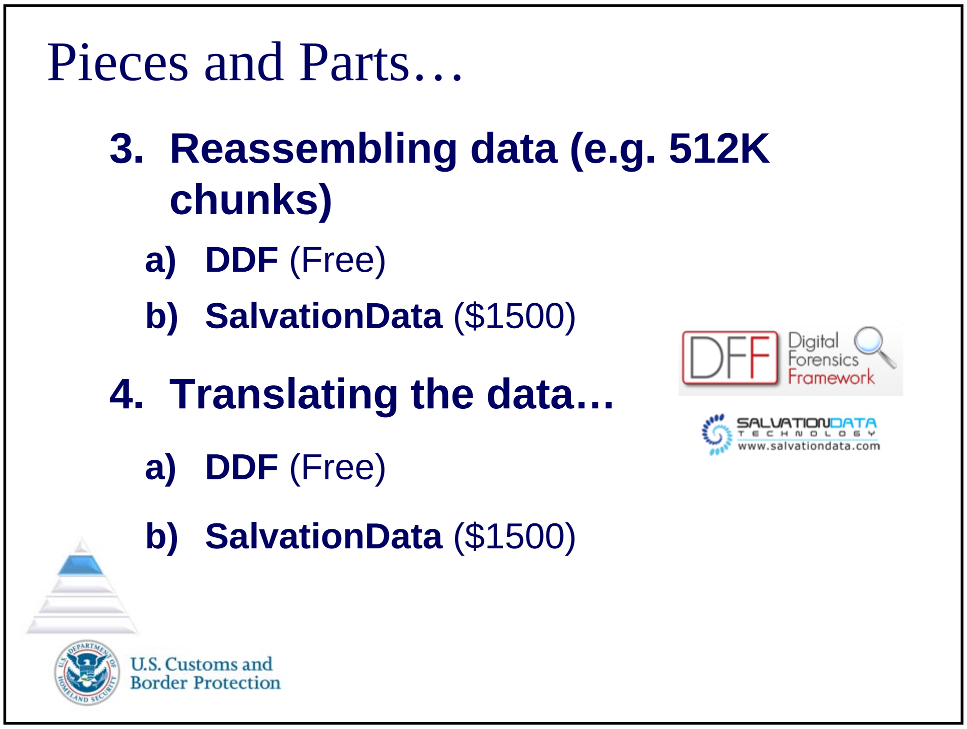
1. **Remove Chip**
   - A. **IRSA IR 550 Plus**
     - ~$20,000
   - B. **Heat Gun**
     - ~$75
   - C. **Soldering Iron**
     - ~$200

2. **Read Chip**
   - A. **FlashPak III**
     - ~$10,000
   - B. **NAND Socket Module**
     - ~$1,500



Cost: $32,000 USD

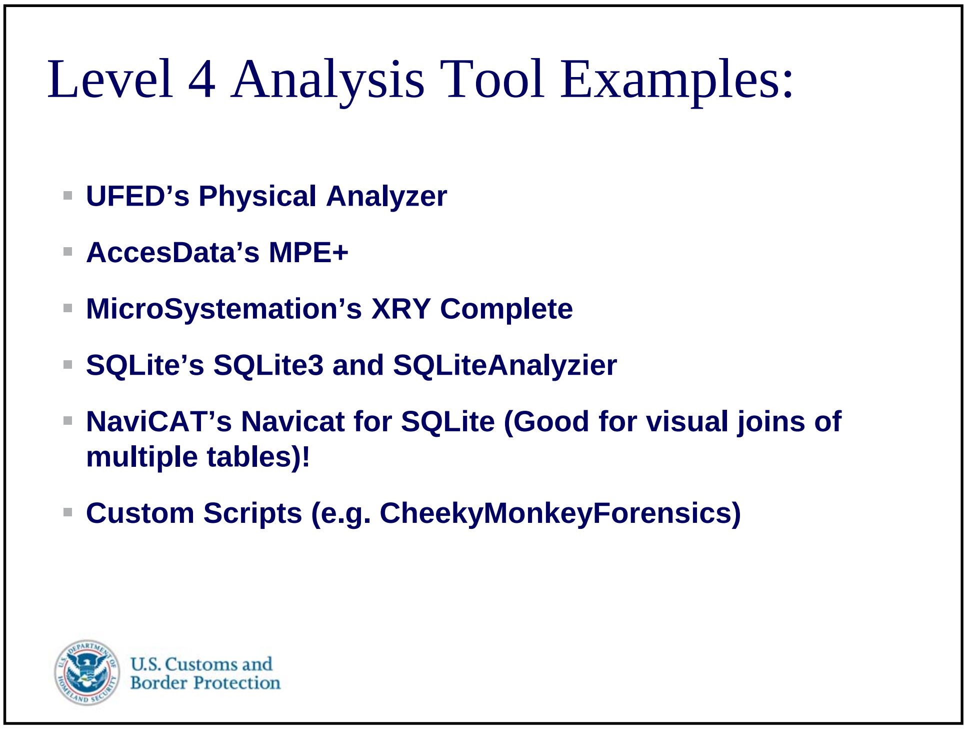
U.S. Customs and Border Protection



Pieces and Parts…

3. **Reassembling data (e.g. 512K chunks)**
   a) **DDF** (Free)
   b) **SalvationData** ($1500)
4. **Translating the data…**
   a) **DDF** (Free)
   b) **SalvationData** ($1500)

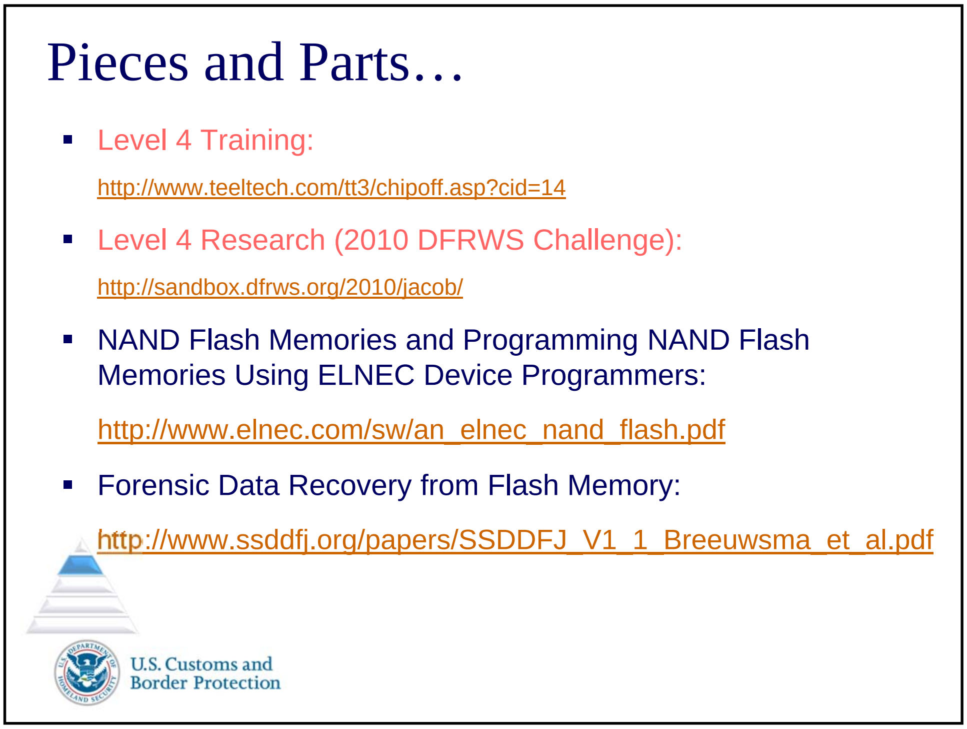
DFF Digital Forensics Framework
SALVATIONDATA TECHNOLOGY
www.salvationdata.com
U.S. Customs and Border Protection



Level 4 Analysis Tool Examples:

- **UFED’s Physical Analyzer**
- **AccesData’s MPE+**
- **MicroSystemation’s XRY Complete**
- **SQLite’s SQLite3 and SQLiteAnalyzier**
- **NaviCAT’s Navicat for SQLite (Good for visual joins of multiple tables)!**
- **Custom Scripts (e.g. CheekyMonkeyForensics)**

U.S. Customs and Border Protection



Pieces and Parts…

- Level 4 Training:

  http://www.teeltech.com/tt3/chipoff.asp?cid=14

- Level 4 Research (2010 DFRWS Challenge):

  http://sandbox.dfrws.org/2010/jacob/

- NAND Flash Memories and Programming NAND Flash Memories Using ELNEC Device Programmers:

  http://www.elnec.com/sw/an_elnec_nand_flash.pdf

- Forensic Data Recovery from Flash Memory:

  http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

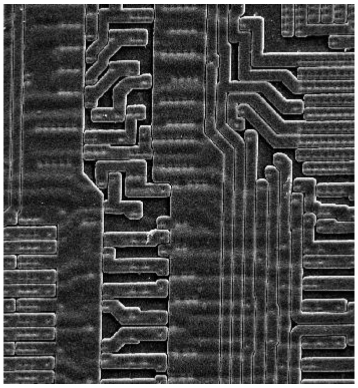
U.S. Customs and Border Protection

Level 5 Tools: (Micro Read)

U.S. Customs and Border Protection

High-Power Microscope

1. Use chemical process to remove top layer of chip
2. Use microscope to read gates manually.
3. Translate binary to hex
4. Translate hex to data



U.S. Customs and Border Protection

Level 5 Tools: (Micro Read)

- “Design Principles for Tamper-Resistant Smartcard Processors”

  http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf
- “Physical NAND Flash Security: Preventing Recovery of Deleted Data”

  http://www.flashmemorysummit.com/English/Collaterals/Proceedings/2011/20110808_PreConf_FSam_Abraham.pdf

U.S. Customs and Border Protection

Other Links:

- NIST: Computer Forensics Tool Testing (CFTT) of Mobile Devices:

  http://www.cftt.nist.gov/mobile_devices.htm

  - Includes: Smart Phones, GSM and Non-GSM Phones
    - Tool Specifications
    - Test Assertions
    - Test Plans
    - Test Results

U.S. Customs and
Border Protection

Contact Info:

- Email:
  - sam.brothers@dhs.gov
- Phone:
  - (703) 921-7149

U.S. Customs and
Border Protection

U.S. Customs and Border Protection