Things I Thought Were Ground Truth in Digital Forensics Until I Found Out I Was Totally Wrong
And What to Do About it Now
Cindy Murphy

- President, Gillware Digital Forensics – 2 years already!!
- Law Enforcement Officer for 31 years
  - Madison Police Department since 1991, Detective for 17+ years
- Involved in Computer Crimes & Computer Forensics 18+ years
  - Certified Computer Forensic Examiner
  - Testified as an Expert in State and Federal Courts
  - D.F. cases in both the WI and US Supreme Court
- Certified Instructor/Co-Author SANS FOR585 – Advanced Mobile Device Forensics
- MSc – University College, Dublin – Forensic Computing and Cybercrime Investigation
Ground Truth.

Direct Observation == Empirical Observation == Fundamental Truth == The Way Things ARE

1. Imaging
2. Firmware
3. Hardware
4. What do we do about it?
1. Imaging:
(As examples go, an oldie but a goodie!)

Reality:
• We get a bit-for-bit image of the user addressable area of the hard drive or memory chip.
Less Accessible Drive Areas:

• Service / System Area:
  • S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology
• Reserved Area
• Servo Information
• Device Configuration Overlay (DCO)
• Host Protected Area (HPA)
• Firmware?!

2. Firmware

Myth:
• Firmware doesn’t matter so long as it works.

Reality:
• Firmware matters.
Firmware

• What is it?
  • Built in software that provide low level control over hardware.
  • Acts as the middle man between hardware and OS

• It’s Everywhere!
  • USB keyboards, web cams, sound cards, graphics cards, computer batteries, cell phones, cell phone base band*, audio recorders, thumb drives, smart TVs, digital cameras, GPS, traffic signals, routers, printers, vehicles, tractors, etc...

Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware
Firmware

• Why does it matter?
  • Can be easily exploited – firmware is not designed for security.
    • Counterfeit USB/SD Devices
    • Meltdown/Spectre
    • Intel AMT Firmware Vulnerability
  • Unlike modern operating systems, firmware rarely has easy update mechanisms.
  • We can use it to help us access devices that otherwise can’t be accessed.
  • Understanding it helps us in the mobile forensics realm – boot loops can be overcome!

3. Hardware:

<table>
<thead>
<tr>
<th>Myth:</th>
<th>Reality:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Hardware doesn’t matter so long as it works.</td>
<td>• Hardware matters.</td>
</tr>
</tbody>
</table>
Hardware

• Hardware might be the last thing we’re thinking of when we’re trying to get to data, but sometimes you just need to go there…

http://dangerousprototypes.com/blog/
Hardware

• Why does it matter?
  • Repairs/Replacement/Reconfiguration can solve problems that other methods can’t.
  • Board swaps, chip, head swaps, etc... for drives
  • Chip swaps, board swaps, etc... for phones
  • Alternative input methods, hardware hacks
A Great Example.

- You image an SD Card from a digital camera through a write protector. The image looks like this from the first bit to the last.

- Are you done with your exam???

- 300+ images would be left behind...
Super simplistic overview:
(Why you shouldn’t believe the card is empty!)

File System

Flash Translation Layer

NAND Flash Memory

Our software based imagers can reach and understand data as it exists here.

The FTL shows us data the way it “should” look, not how it actually is.

Until it’s actually overwritten or cleaned up by garbage collection/wear leveling your data still lives here!
There’s more than meets the eye...

- With Flash Memory Devices there are two avenues to data extraction:
  - Normal Device Interface – SATA, eMMC, SDIO, etc...
  - Direct read of NAND Flash – one or more chips
Peeling away the FTL Curtain...

- Chip off or direct read of the NAND
- There’s data there!
- Will need to do some significant puzzle work.
So, Why Not Just Always read the NAND Directly?

- Individual NAND flash memory chips employ an industry-standard interface
- Reader hardware can be found for a couple hundred dollars
- Seems pretty straight forward…
Not so straight forward:

- It’s difficult to impossible to make use of data read directly from NAND
- Most modern SSDs encrypt with AES-128/256
- Must manually determine FTL logical-to-physical mapping
- Wear leveling can leave behind hundreds of previous revisions for any given LBA
- Data is useless until proprietary error-correction routine is performed
- Physically destructive to the original device
What do we do about it?

• Keep learning, reaching, and growing.
• Adjust as you go.
• When your understanding changes, share!
Questions?
gillware.com/forensics
cmurphy@gillware.com