Damaged Device Forensics
An update on a U.S. Department of Homeland Security R&D Project

Steve Watson, Principal Investigator
Acknowledgement & Disclaimer

This material is based on research sponsored by the United States Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) via contract number HHSP233201700021C.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security.
Customer Need

- Law enforcement agencies receive electronic devices as evidence that have endured physical damage to the device.
- Most agencies do not receive damaged devices frequently enough to develop expertise in how to address damaged devices.
- Limited research has been focused on data acquisition from damaged devices.
- Data retrieval from devices still needed.
Approach (Part 1)

Introduce physical damage to the device along four damage methodologies that agencies are receiving.

1. Liquid Damage
2. Thermal Damage
3. Ballistics Damage
4. Impact Damage
Approach (Part 2)

• Damage will be inflicted on devices in similar ways to real-world scenarios.

• Effect of the damage on devices will be identified.

• Scientific instruments and protocols will be used to measure the effects of damage on the devices.
Approach (Part 3)

• Methods for addressing each stage of a damaged device will be identified.

• Methods to achieve data acquisition from damaged devices will be identified.

• Identification of catastrophic damage where data acquisition is no longer possible will be sought.
Benefits

• Baseline scientific research on all exhaustive methods for data acquisition from damaged devices.

• Protocols to be developed and shared for successfully dealing with damaged devices across multiple damage methodologies.

• Support for law enforcement to incorporate damage device protocols into their existing standard operating procedures.
Process

• Each damage modality includes a series of individual studies that complement or build upon each other.

• All studies are focused on the viability of data acquisition.

• Results from each discreet study are written to capture results.

• Practice based outcome will identify best practices.
Competition

• Existing industry practices:
  • Many industry practices are anecdotal at best with no identified science backing the ‘best practice’ claims.

• Research:
  • Disparate protocols exist across numerous industries but has not been reconciled for digital forensics and data recovery.

  • Damaged Device project builds on last few years of PI’s work in this space.
Liquid Damage

2. Submersion Longevity Study.
Liquid Damage


7. Application of Liquid Recovery Plan Against CONUS Water Samples.
Liquid Damage
Recent Test
Hygroscopic Capacity of Integrated Circuit Packages and Printed Circuit Boards
Terms

• integrated circuit packages

• circuit boards

• hygroscopic capacity

• hygroscopic coefficient
Hypothesis

• Will chips and circuit boards exposed to liquids absorb an increasing amount of liquid?

• Can a maximum absorption level be identified?
<table>
<thead>
<tr>
<th></th>
<th>0 % RH</th>
<th>20% RH</th>
<th>66% RH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chips</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% weight change</td>
<td>0.1787%</td>
<td>0.1228%</td>
<td>0.1275%</td>
</tr>
<tr>
<td>% moisture content</td>
<td>0.1780%</td>
<td>0.1225%</td>
<td>0.1265%</td>
</tr>
<tr>
<td>Mean</td>
<td>0.1252%</td>
<td>0.1250%</td>
<td>0.0576%</td>
</tr>
<tr>
<td>Median</td>
<td>0.1253%</td>
<td>0.1035%</td>
<td>0.0575%</td>
</tr>
<tr>
<td>PCBs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% weight change</td>
<td>1.3114%</td>
<td>0.6167%</td>
<td>0.5755%</td>
</tr>
<tr>
<td>% moisture content</td>
<td>1.2693%</td>
<td>0.6073%</td>
<td>0.5636%</td>
</tr>
<tr>
<td>Mean</td>
<td>0.8329%</td>
<td>0.4343%</td>
<td>0.5612%</td>
</tr>
<tr>
<td>Median</td>
<td>0.8260%</td>
<td>0.4324%</td>
<td>0.4851%</td>
</tr>
</tbody>
</table>
Results – Duration Absorption

Integrated Circuit Packages

0%RH, 20%RH, 66%RH

Linear (0%RH), Linear (20%RH), Linear (66%RH)
Conclusion

• Hygroscopic capacity of integrated circuit packages and printed circuit boards confirmed through methodical observation.

• Understanding that device components can absorb liquid should inform practitioners when addressing devices exposed to liquid.

• Pre-submersion humidity levels may have previously unrecognized effects as well.
Liquid Takeaways

• The makeup of the liquid has a significant impact on damage to device.

• Devices should be transported in liquid from scene to lab.

• Devices should be addressed as soon as possible.

• Wet devices need to be dried before any work begins.
Thermal Update

1. Thermal Damage (Baseline). Completed.
Thermal Takeaways

- Devices are far more resilient than most agencies realize.
- Temperatures so far 900-1000 degrees with successful acquisitions.
- Expect challenges open up melted devices.
- Expect chips to be desoldered from the board.
Impact Update

Impact Damage Paper

1. Samsung Solstice II (SGH-A817)
   • 70 grams (2.47 ounces) w/o battery; 91 grams (3.21 ounces) w/ battery

2. Terminal Velocity
   • Weight / Gravity / Air Density / Atmospheric Pressure / Temperature / Area of the object / Drag Coefficient
   • 34.51 mph

3. Impact
   • G-Force: **157 G’s**
   • Equivalent of **36,110 lbs** hitting **230 lb body** for 0.1 second
Ballistics Update

1. Firearms Damage (Sidearm Calibers) Completed.


3. Explosive Damage (Baseline). Local agency collaboration identified.
Impact of Projectile in ft/lbs
Ballistic Takeaways

• If the projectile goes through the flash, the possibility of data retrieval is gone.

• If the projectile hits somewhere else on the board, the likelihood of retrieving data via chip-off increases.

• We have not yet identified a ballistics impact that damaged inside the chip.
Further Research Questions

• Intra IC Package Data Acquisitions via Bond Wire and Die

• Understanding the Efficacy of IC Package Removal and Successful Acquisition by Standard Labs

• The Application of Failure Analysis Techniques to Determine the Acquisition Failure from IC Packages