Damaged Device Forensics

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

Steve Watson, Principal Investigator

VTO Labs

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.

VTO Labs

VTO Labs

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.

VTO Labs

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

VTO Labs

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.

VTO Labs

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.

VTO Labs

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.

VTO Labs

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.

VTO Labs

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.

VTO Labs

Liquid Damage

1. Hygroscopic Capacity of Integrated Circuit Packages and Printed Circuit Boards.
2. Submersion Longevity Study.
3. Efficacy of Cleaning Techniques.
4. Efficacy of Drying Techniques.

VTO Labs

Liquid Damage

5. Biohazard Protocol Definition.

6. Flammable Liquid Protocol Definition.

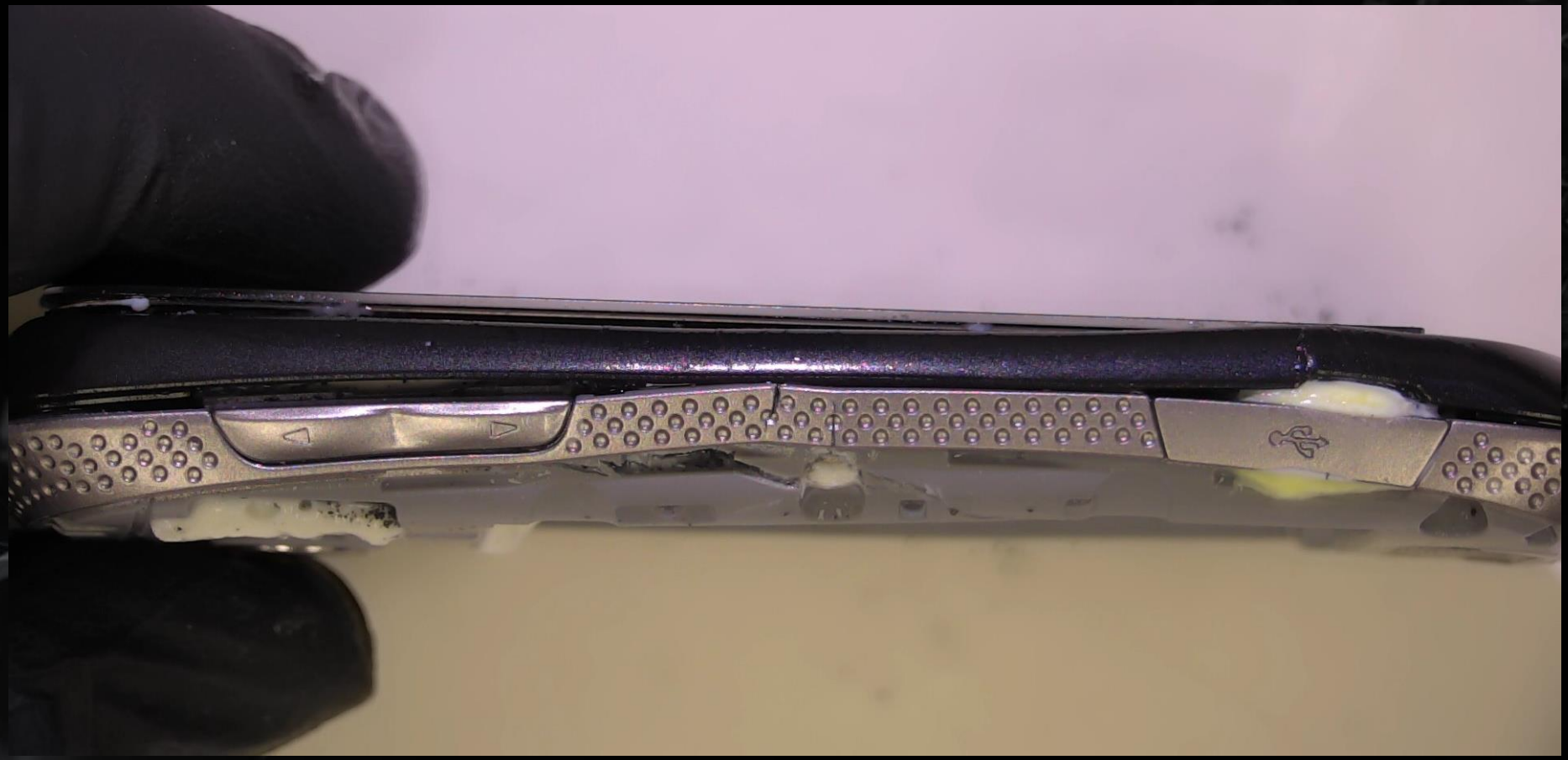
7. Application of Liquid Recovery Plan Against CONUS Water Samples.

VTO Labs

Liquid Damage

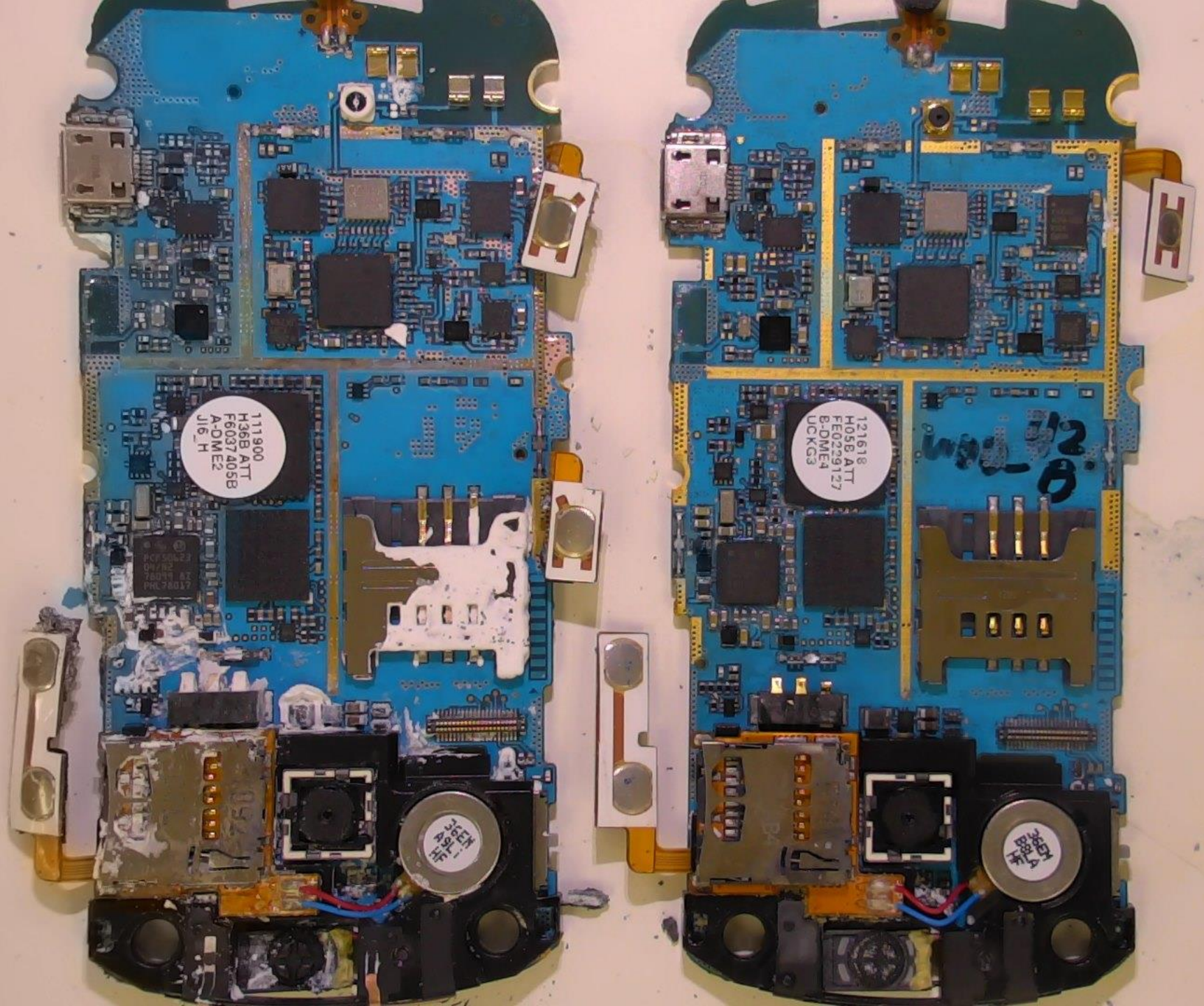
VTO Labs

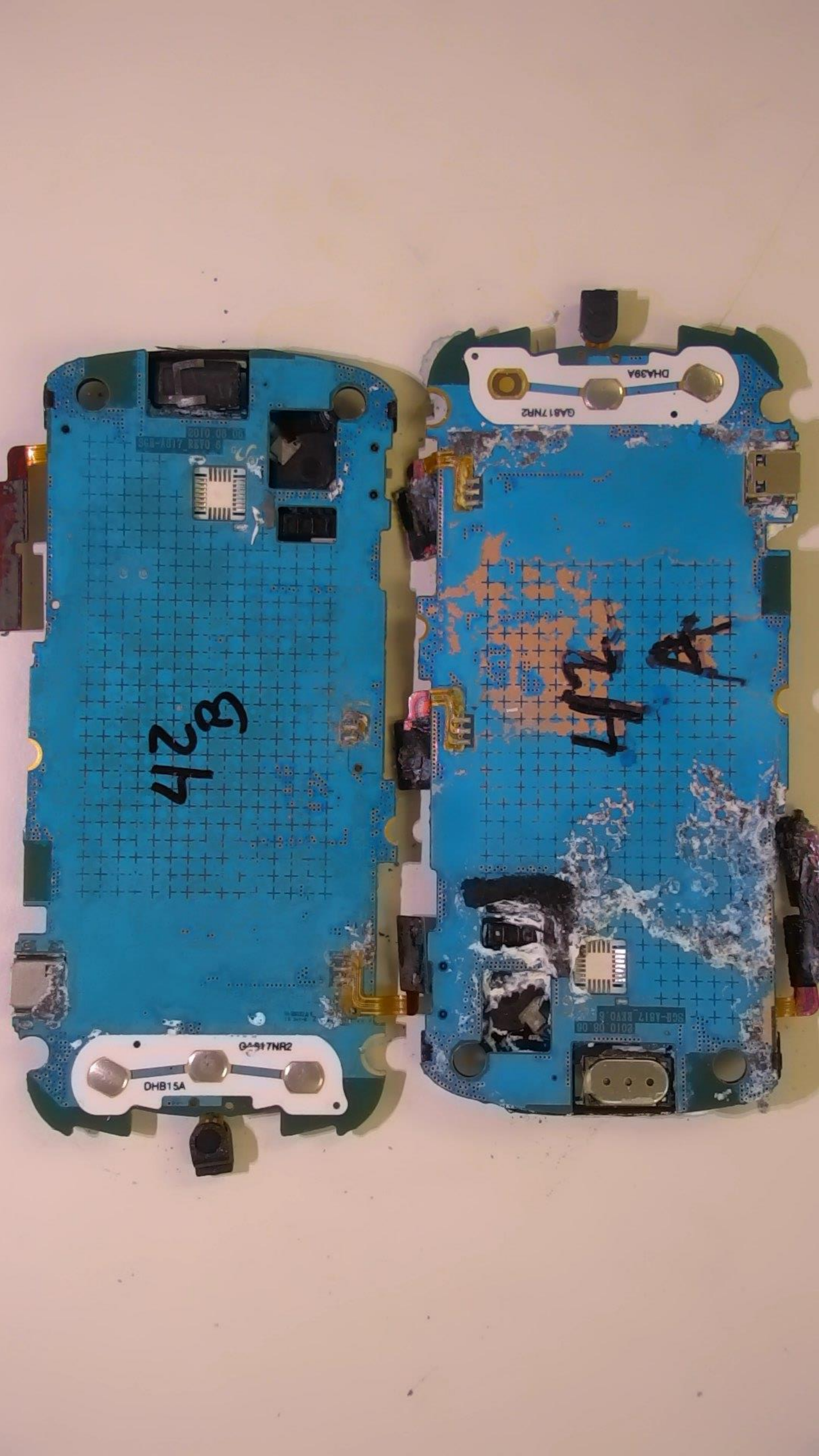
Recent Test



VTO Labs

IMEI: 364493041435370
S/N: ROHZB366477
SKU: 65202
MADE IN CHINA
REV1.0
CE 0168


111900
H36B ATT
F6037405B
A-DME2
JI6_H
121618
H05B ATT
FE0229127
B-DME4
UCKG3


428
DHB15A
GA817NR2
DHA39A
GA817NR2

Hygroscopic Capacity of Integrated Circuit Packages and Printed Circuit Boards

VTO Labs

Terms

- integrated circuit packages
- circuit boards
- hygroscopic capacity
- hygroscopic coefficient

VTO Labs

Hypothesis

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

- Can a maximum absorption level be identified?

VTO Labs

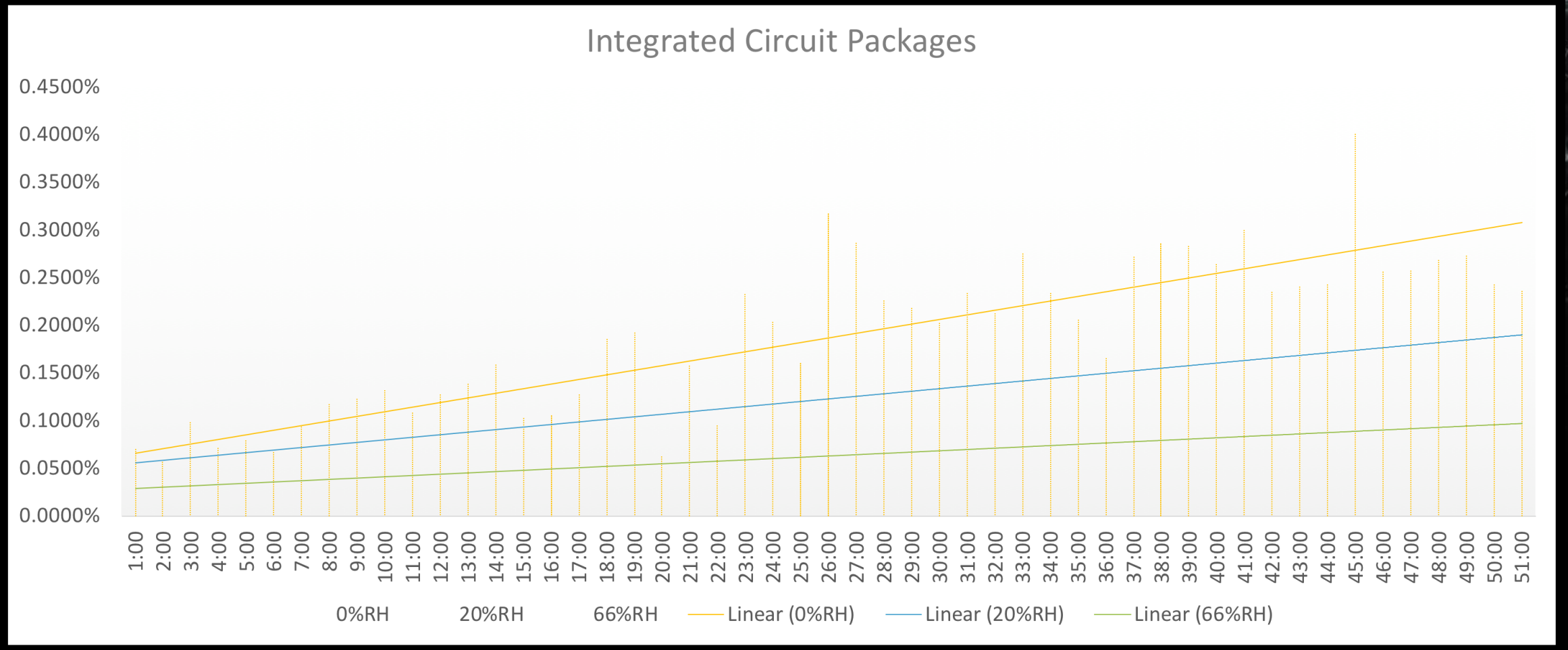
Results – 10 hour median and mean

Chips	0 % RH		20% RH		66% RH	
	% weight change	% moisture content	% weight change	% moisture content	% weight change	% moisture content
Mean	0.1787%	0.1780%	0.1228%	0.1225%	0.1275%	0.1265%
Median	0.1252%	0.1250%	0.1035%	0.1034%	0.0576%	0.0575%

PCBs	0 % RH		20% RH		66% RH	
	% weight change	% moisture content	% weight change	% moisture content	% weight change	% moisture content
Mean	1.3114%	1.2693%	0.6167%	0.6073%	0.5755%	0.5636%
Median	0.8329%	0.8260%	0.4343%	0.4324%	0.5612%	0.4851%

VTO Labs

Results – Duration Absorption



VTO Labs

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.

VTO Labs

Liquid Takeaways

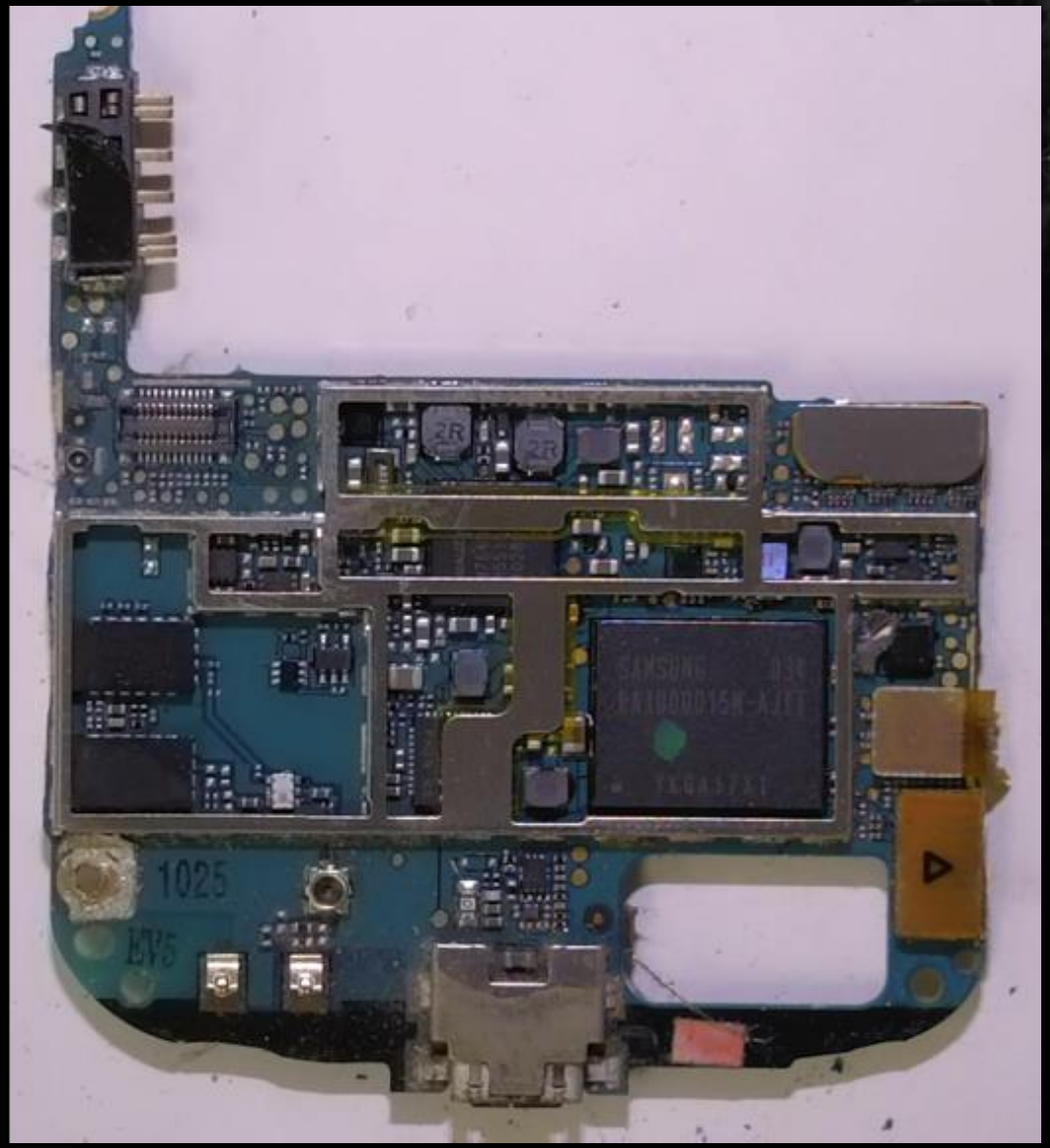
- The makeup of the liquid has a significant impact on damage to device.
- Devices should be transported in liquid from scene to lab.
- Devices should be addressed as soon as possible.
- Wet devices need to be dried before any work begins.

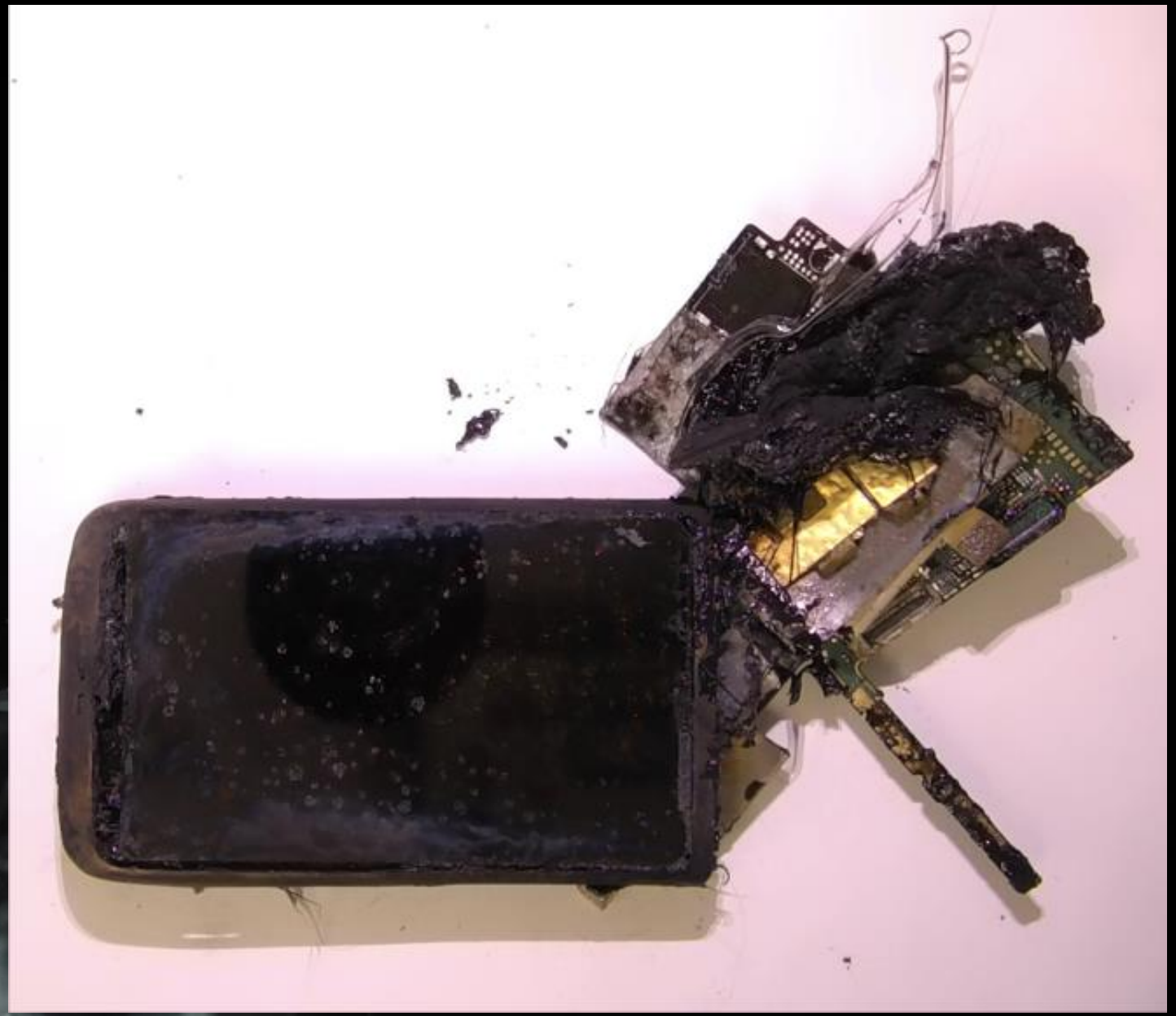
VTO Labs

Thermal Update

1. Thermal Damage (Baseline). Completed.
2. Thermal Damage (Expansion). Scheduled.
3. Microwave Damage. Completed. Paper in draft.
4. Potential damage from fire suppression foams. Completed. Paper finalized.

VTO Labs





VTO Labs

DAMAGED MOBILE DEVICE FORENSICS
VTO INC

VTO Labs

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.

VTO Labs

Impact Update

1.Impact Damage. Completed. Paper finalized.

VTO Labs

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

VTO Labs

Ballistics Update

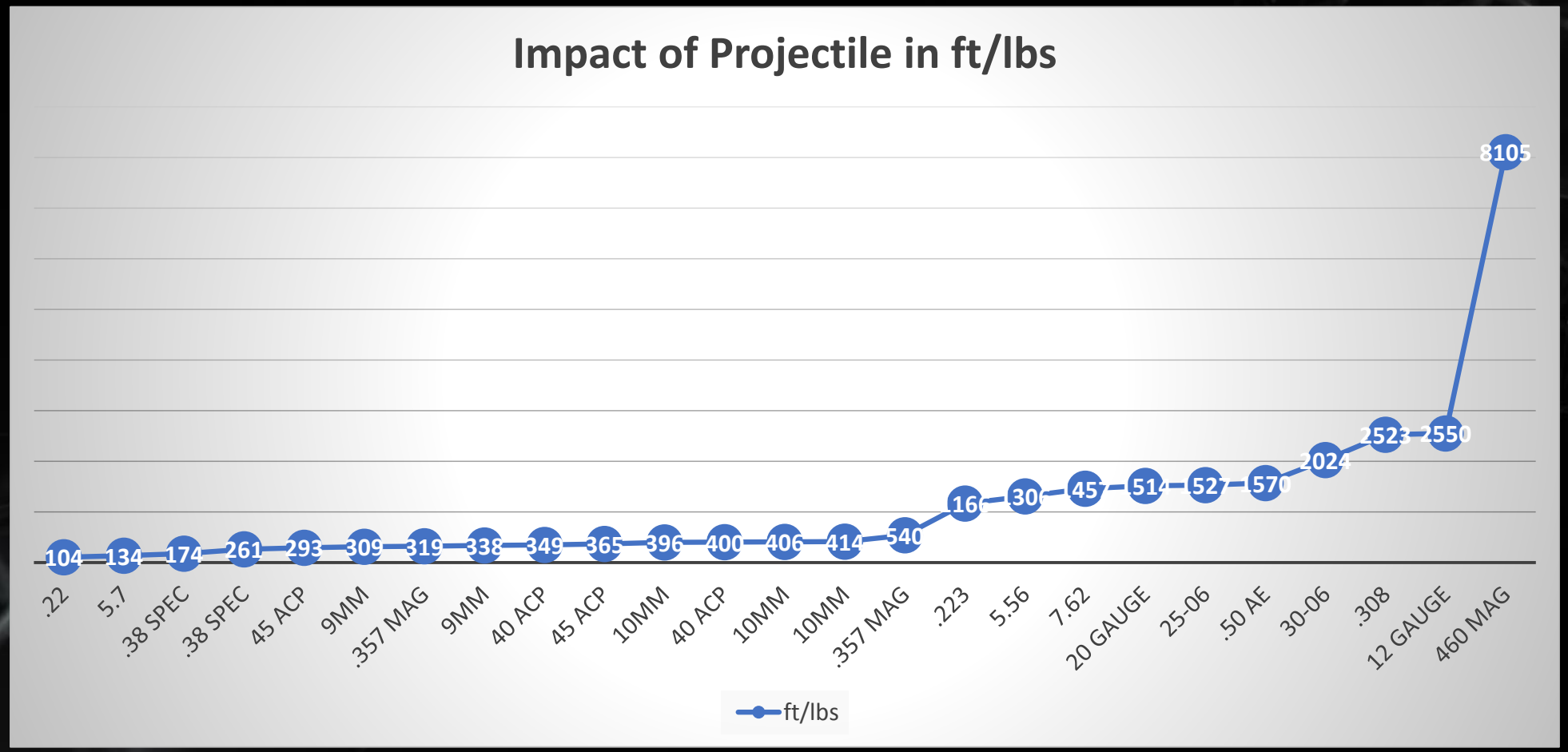
1. Firearms Damage (Sidearm Calibers) Completed.

2. Firearms Damage (Long gun Calibers) Completed. Paper in draft.

3. Explosive Damage (Baseline). Local agency collaboration identified.

VTO Labs

Ballistics Damage Paper



VTO Labs

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.

VTO Labs

Summary

13 PAPERS

VTO Labs

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

VTO Labs

VTO Labs

stevewatson@vtolabs.com