Flash Memory Summit

Improving Chip-Off Forensic Analysis for NAND Flash

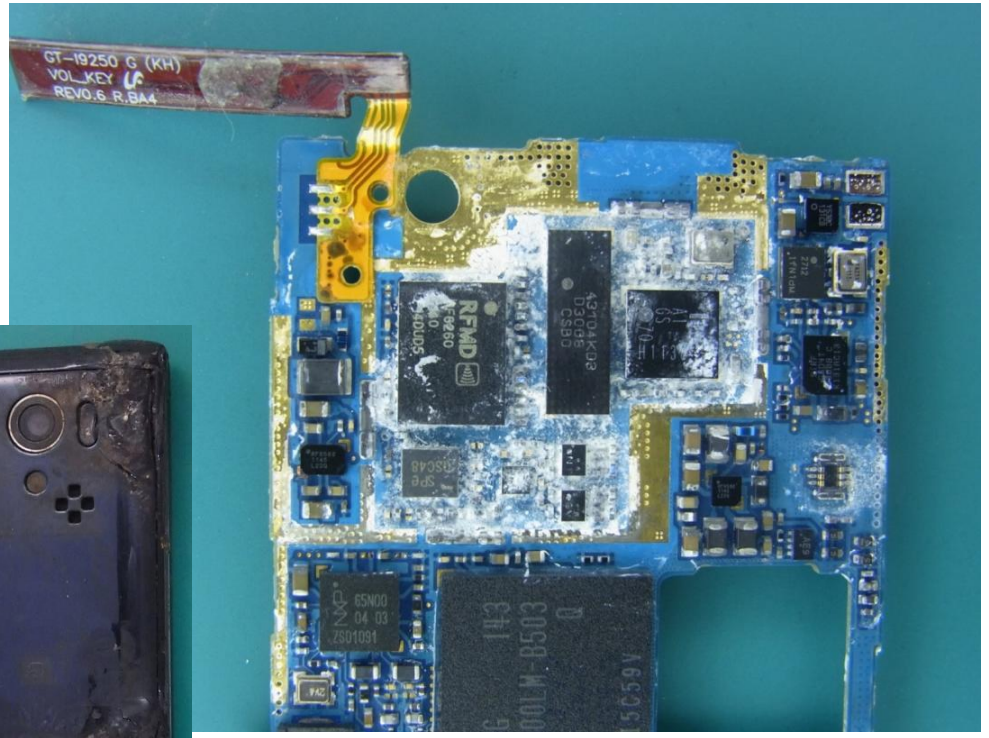
Challenges Law Enforcement Organizations are Facing

Aya Fukami
(fukami@post.cyberpolice.go.jp)

Carnegie Mellon University
National Police Agency of Japan

Flash Memory Summit

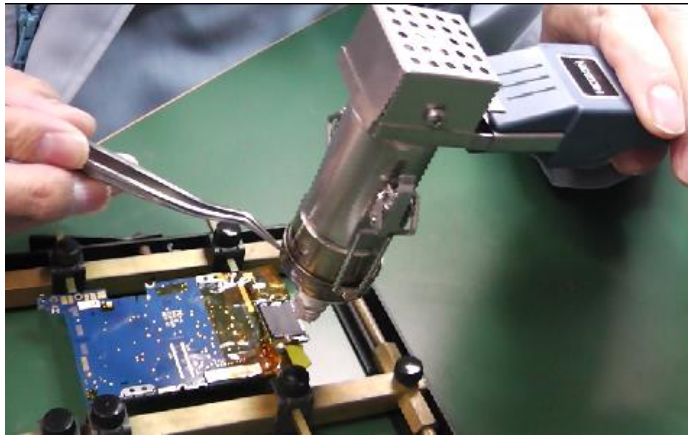
Digital Forensics

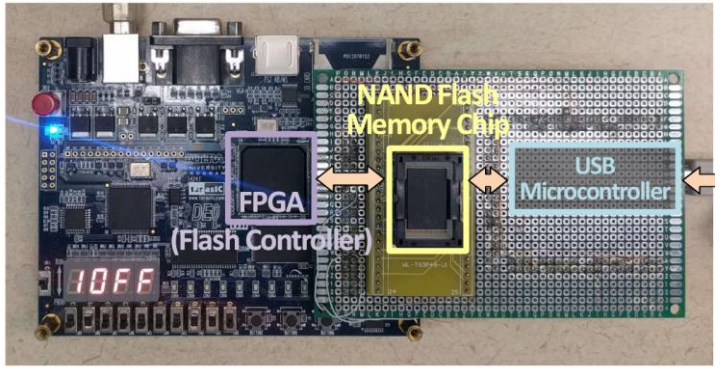


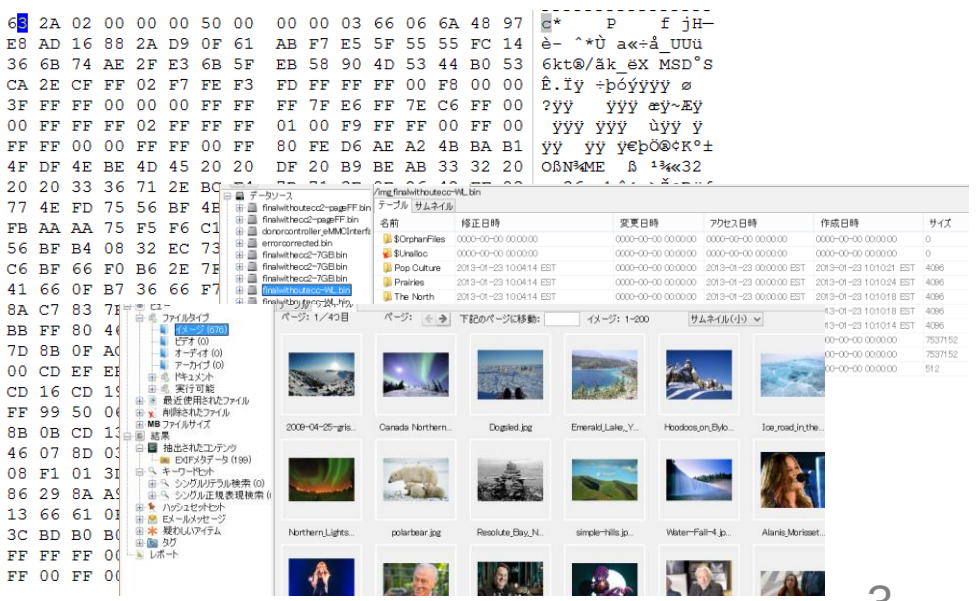
Recovering data from these kinds of devices for criminal investigations

“Chip-off” Forensic Analysis

Chip removal → Data Extraction → Data Analysis



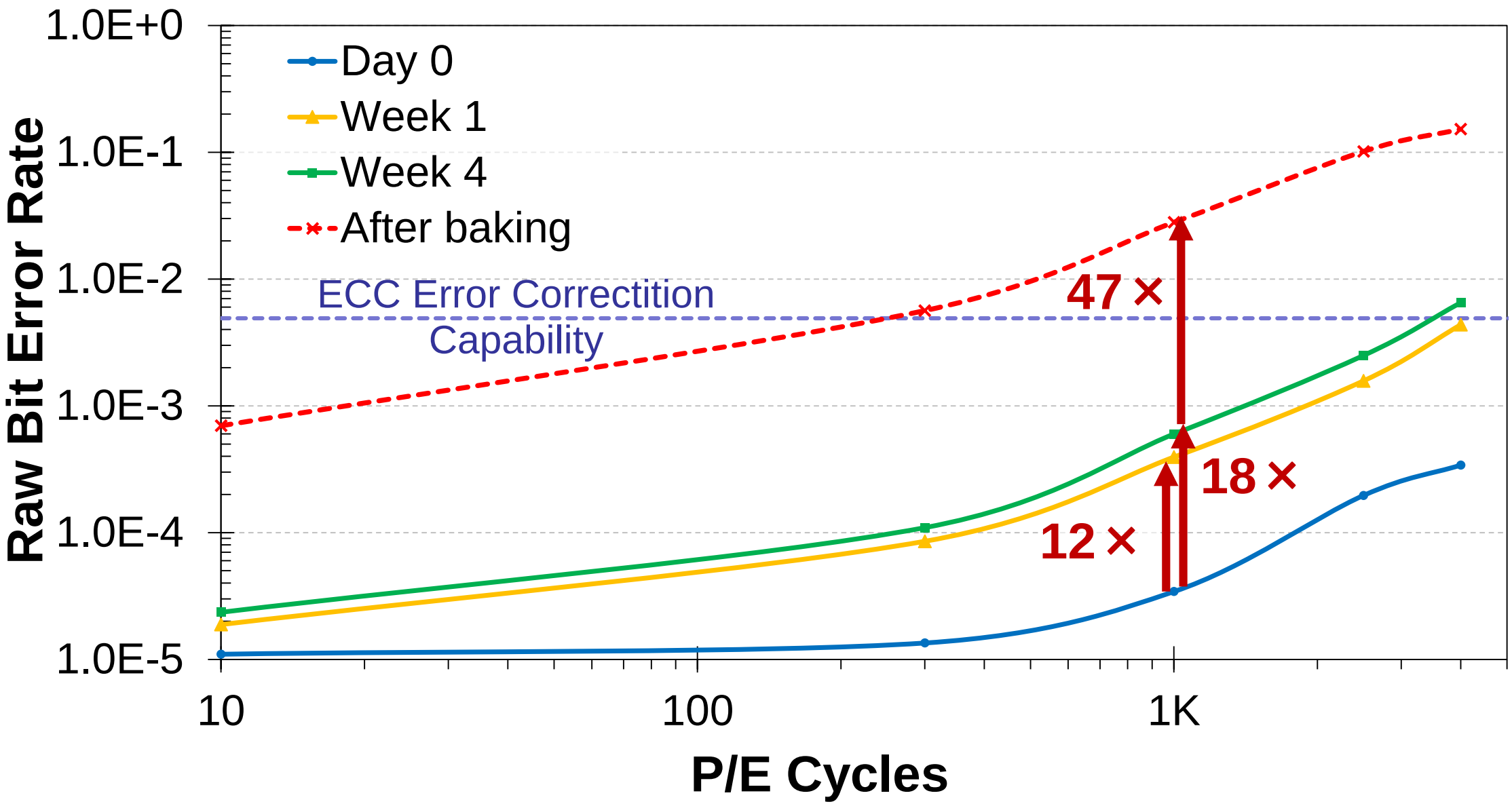




Challenges in Chip-off Analysis

- Retention error: Backlogs in DF labs can be over a year
- Bit errors introduced by heat: Heat applied during chip removal from PCB: more bit errors
- Reverse engineering ECC & randomization algorithm: Required for file system reconstruction: usually no information available about controllers

Challenges in Chip-off Analysis



Recent Improvement in Chip-Off Analysis

- Exploiting read-retry operation (Fukami et al. Improving the reliability of chip-off forensic analysis of NAND flash memory devices, DFRWS EU 2017 [Best paper award])
- Non-thermal chip removal: lapping out PCB from the bottom (Billard and Vidonne, “Chip-off by matter subtraction: frigida via”, SADFE 2016)
- Utilizing Berlekamp-Massey algorithm for LFSR parameter identification (Zandwijk “A mathematical approach to NAND flash-memory descrambling and decoding”, Digital Investigation 2015)

We All Win When We Work Together

- New technologies (Xpoint, 3D NAND, LDPC etc.) = Greater digital forensics challenges
- Thermal effect to NAND flash memory data can be explored more
- Forensics research can be also beneficial for NAND flash memory reliability research

Thank you!

Improving Chip-Off Forensic Analysis for NAND Flash

Challenges Law Enforcement Organizations are Facing

Aya Fukami
(fukami@post.cyberpolice.go.jp)
Carnegie Mellon University
National Police Agency of Japan

References to Papers and Talks

- Saugata Ghose, Vulnerabilities in MLC NAND Flash Memory Programming, FMS 2017
- Onur Mutlu, ThyNVM: Software-Transparent Crash Consistency for Persistent Memory, FMS 2016.
- Onur Mutlu, Large-Scale Study of In-the-Field Flash Failures, FMS 2016.
- Yixin Luo, Practical Threshold Voltage Distribution Modeling, FMS 2016.
- Saugata Ghose, Write-hotness Aware Retention Management, FMS 2016.
- Onur Mutlu, Read Disturb Errors in MLC NAND Flash Memory, FMS 2015.
- Yixin Luo, Data Retention in MLC NAND Flash Memory, FMS 2015.
- Onur Mutlu, Error Analysis and Management for MLC NAND Flash Memory, FMS 2014.
- FMS 2017 posters (Booth 833):

  Accurate and Practical Online Flash Channel Modeling for MLC NAND Flash

  Vulnerabilities in MLC NAND Flash Programming: Analysis, Exploits, and Mitigation

  Error Characterization, Mitigation, and Recovery in Flash Memory Based SSDs

Flash Memory Works at Carnegie Mellon University

- Summary of our work in NAND flash memory
  - **Yu Cai, Saugata Ghose, Erich F. Haratsch, Yixin Luo, and Onur Mutlu, Error Characterization, Mitigation, and Recovery in Flash Memory Based Solid-State Drives, *Proceedings of the IEEE*, Sept. 2017**
- Overall flash error analysis
  - Yu Cai, Erich F. Haratsch, Onur Mutlu, and Ken Mai, Error Patterns in MLC NAND Flash Memory: Measurement, Characterization, and Analysis, DATE 2012.
  - Yu Cai, Gulay Yalcin, Onur Mutlu, Erich F. Haratsch, Adrian Cristal, Osman Unsal, and Ken Mai, Error Analysis and Retention-Aware Error Management for NAND Flash Memory, ITJ 2013.
  - Yixin Luo, Saugata Ghose, Yu Cai, Erich F. Haratsch, and Onur Mutlu, Enabling Accurate and Practical Online Flash Channel Modeling for Modern MLC NAND Flash Memory, *IEEE JSAC*, Sept. 2016

Flash Memory Works at Carnegie Mellon University

- Flash-based SSD prototyping and testing platform
  - Yu Cai, Erich F. Haratsh, Mark McCartney, Ken Mai, FPGA-based solid-state drive prototyping platform, FCCM 2011.
- Retention noise study and management
  - Yu Cai, Gulay Yalcin, Onur Mutlu, Erich F. Haratsch, Adrian Cristal, Osman Unsal, and Ken Mai, Flash Correct-and-Refresh: Retention-Aware Error Management for Increased Flash Memory Lifetime, ICCD 2012.
  - Yu Cai, Yixin Luo, Erich F. Haratsch, Ken Mai, and Onur Mutlu, Data Retention in MLC NAND Flash Memory: Characterization, Optimization and Recovery, HPCA 2015.
  - Yixin Luo, Yu Cai, Saugata Ghose, Jongmoo Choi, and Onur Mutlu, WARM: Improving NAND Flash Memory Lifetime with Write-hotness Aware Retention Management, MSST 2015.
  - Aya Fukami, Saugata Ghose, Yixin Luo, Yu Cai, and Onur Mutlu, Improving the Reliability of Chip-Off Forensic Analysis of NAND Flash Memory Devices, *Digital Investigation*, Mar. 2017.

Flash Memory Works at Carnegie Mellon University

- Program and erase noise study
  - Yu Cai, Erich F. Haratsch, Onur Mutlu, and Ken Mai, Threshold Voltage Distribution in MLC NAND Flash Memory: Characterization, Analysis and Modeling, DATE 2013.
  - Y. Cai, S. Ghose, Y. Luo, K. Mai, O. Mutlu, and E. F. Haratsch, Vulnerabilities in MLC NAND Flash Memory Programming: Experimental Analysis, Exploits, and Mitigation Techniques, HPCA 2017.
- Cell-to-cell interference characterization and tolerance
  - Yu Cai, Onur Mutlu, Erich F. Haratsch, and Ken Mai, Program Interference in MLC NAND Flash Memory: Characterization, Modeling, and Mitigation, ICCD 2013.
  - Yu Cai, Gulay Yalcin, Onur Mutlu, Erich F. Haratsch, Osman Unsal, Adrian Cristal, and Ken Mai, Neighbor-Cell Assisted Error Correction for MLC NAND Flash Memories, SIGMETRICS 2014.

Flash Memory Works at Carnegie Mellon University

- Read disturb noise study
  - Yu Cai, Yixin Luo, Saugata Ghose, Erich F. Haratsch, Ken Mai, and Onur Mutlu, Read Disturb Errors in MLC NAND Flash Memory: Characterization and Mitigation, DSN 2015.
- Flash errors in the field
  - Justin Meza, Qiang Wu, Sanjeev Kumar, and Onur Mutlu, A Large-Scale Study of Flash Memory Errors in the Field, SIGMETRICS 2015.
- Persistent memory
  - Jinglei Ren, Jishen Zhao, Samira Khan, Jongmoo Choi, Yongwei Wu, and Onur Mutlu, ThyNVM: Enabling Software-Transparent Crash Consistency in Persistent Memory Systems, MICRO 2015.