2k19. Yet Another Cold-Boot Attack

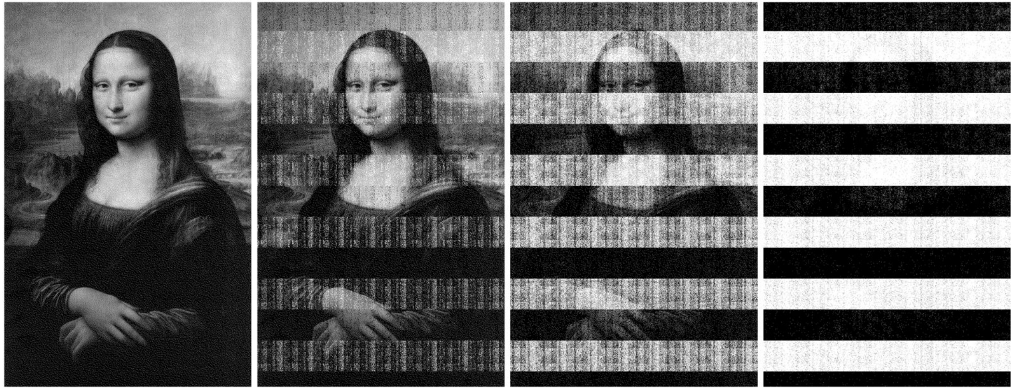
Il’ya Sukhoplyuev
Security & Network Engineering

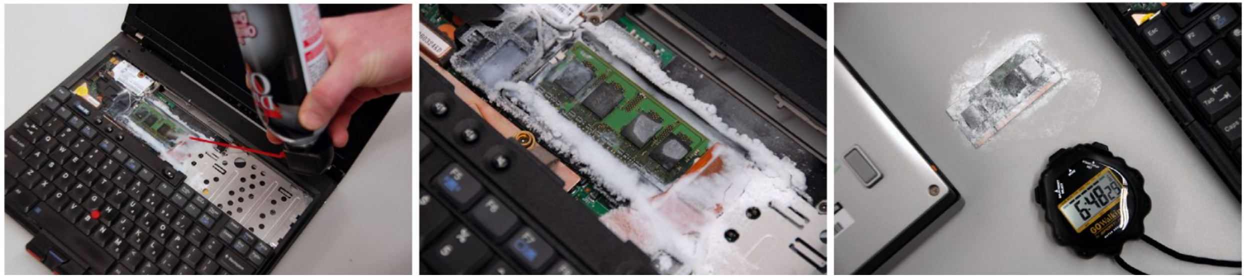
INNOPOLIS UNIVERSITY

April - May 2019

Lest We Remember:
Cold Boot Attacks on Encryption Keys

Halderman and team, USENIX Security Symposium (2008), pdf





Objective

Reproduce
RAM memory dumping
on our equipment

Targets

1. Explore results of “Lest We Remember”

Targets

1. Explore results of “Lest We Remember”
2. Explore DIMM DRAM specifications

Targets

1. Explore results of “Lest We Remember”
2. Explore DIMM DRAM specifications
3. Repeat with published tools set
    a. on Virtual Machine

Targets

1. Explore results of “Lest We Remember”
2. Explore DIMM DRAM specifications
3. Repeat with published tools set
    a. on Virtual Machine
    b. on Real Hardware

Targets

1. Explore results of “Lest We Remember”
2. Explore DIMM DRAM specifications
3. Repeat with published tools set
    a. on Virtual Machine
    b. on Real Hardware
4. Try to create own *Memory Scraper*

Targets

1. Explore results of “Lest We Remember”
2. Explore DIMM DRAM specifications
3. Repeat with published tools set
    a. on Virtual Machine
    b. on Real Hardware
4. **[Work In Progress]** ~~Create Memory Scraper~~

Experiments

Breaking BitLocker on VirtualBox

1. Deploy VM with Windows 10
2. Encrypt Disk with BitLocker
3. Dump the RAM:

    a. `VBoxManage debugvm "WinDev1903Eval" dumpvmcore --filename dump.ram`

Breaking BitLocker on VirtualBox

1. Deploy VM with Windows 10
2. Encrypt Disk with BitLocker
3. Dump the RAM:
    a. `VBoxManage debugvm "WinDev1903Eval" dumpvmcore --filename dump.ram`
4. Find AES keys:
    a. `scripts/coldboot-attacks/bin/aeskeyfind dump.ram`
    b. `4ffa2b21ca45676f321739cef00db137`
    c. `bd91534fca3e27b74969b8c7dc856805`

Breaking BitLocker on VirtualBox

1. Deploy VM with Windows 10
2. Encrypt Disk with BitLocker
3. Dump the RAM:

```
a.  VBoxManage debugvm "WinDev1903Eval" dumpvmcore --filename dump.ram
```

4. Find AES keys:

```
a.  scripts/coldboot-attacks/bin/aeskeyfind dump.ram
b.  4ffa2b21ca45676f321739cef00db137
c.  bd91534fca3e27b74969b8c7dc856805
```

5. Load with Ubuntu Mate:

```
a.  sudo apt-get install libbde-utils
b.  sudo bdemount -k
    4ffa2b21ca45676f321739cef00db137:bd91534fca3e27b74969b8c7dc856805\
c.  /dev/sda2 /mnt
d.  sudo mount -t ntfs -o ro /mnt/bde1 /media
```

Breaking BitLocker on VirtualBox

1. Deploy VM with Windows 10
2. Encrypt Disk with BitLocker
3. Dump the RAM:

```
a.  VBoxManage debugvm "WinDev1903Eval" dumpvmcore --filename dump.ram
```

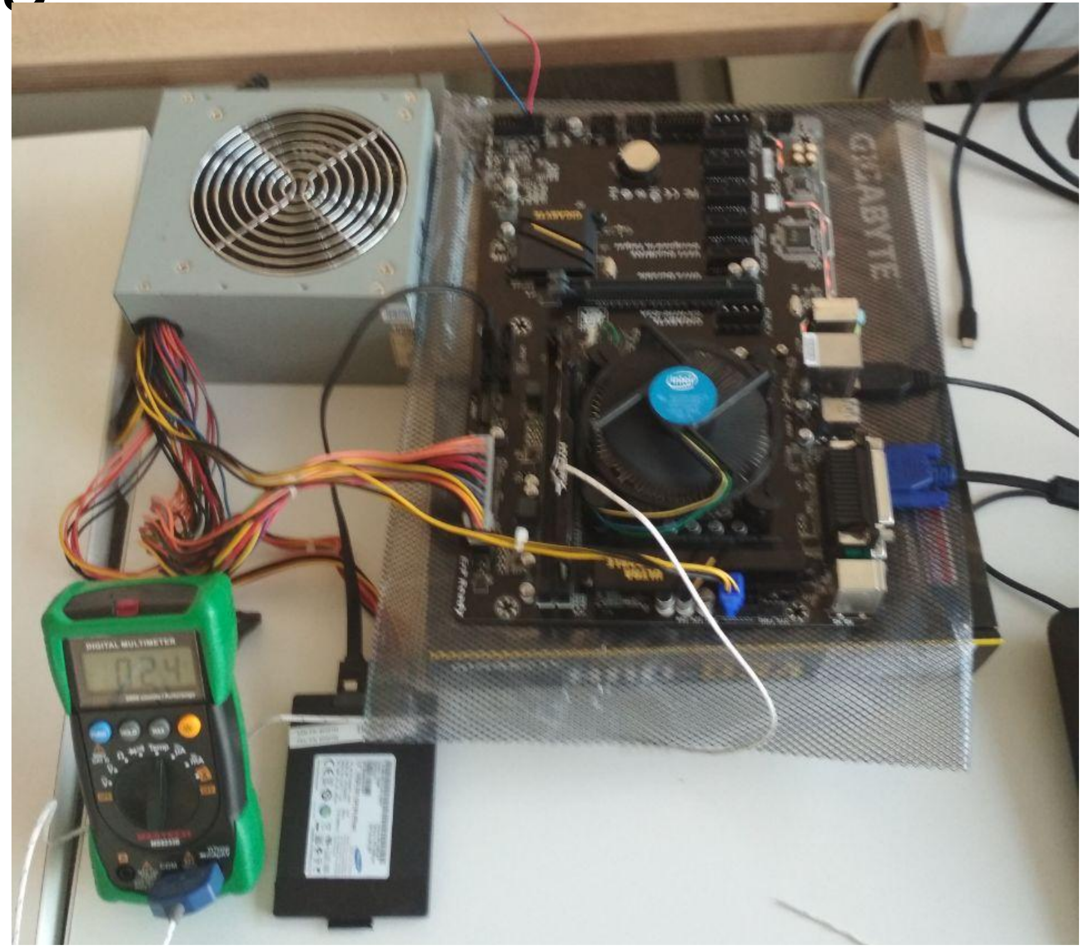
4. Find AES keys:

```
a.  scripts/coldboot-attacks/bin/aeskeyfind dump.ram
b.  4ffa2b21ca45676f321739cef00db137
c.  bd91534fca3e27b74969b8c7dc856805
```

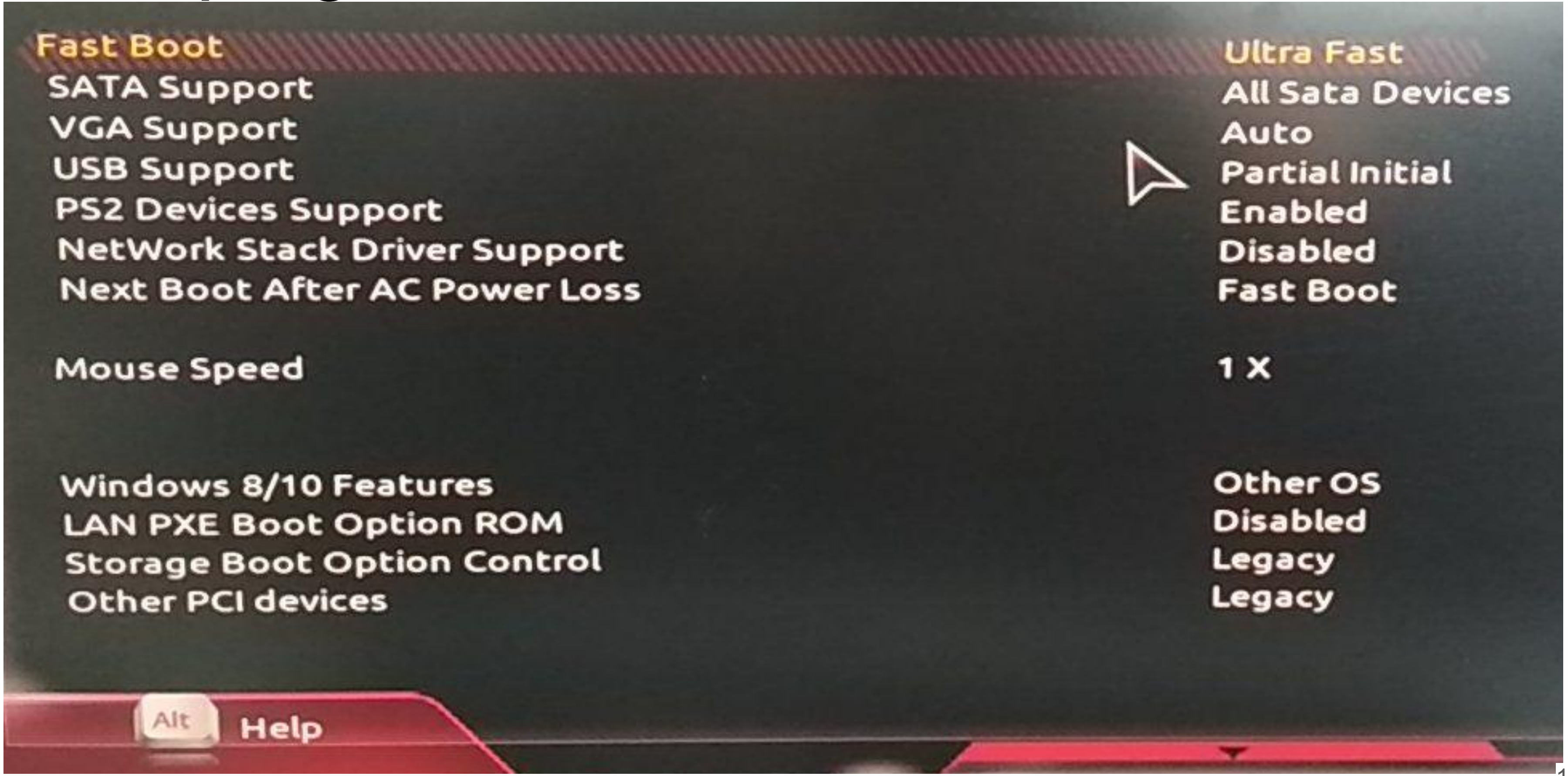
5. Load with Ubuntu Mate:

```
a.  sudo apt-get install libbde-utils
b.  sudo bdemount -k
    4ffa2b21ca45676f321739cef00db137:bd91534fca3e27b74969b8c7dc856805\
c.  /dev/sda2 /mnt
d.  sudo mount -t ntfs -o ro /mnt/bde1 /media
```

Dumping on ~~Bare~~ Brutal Metal



Dumping on ~~Bare~~ Brutal Metal

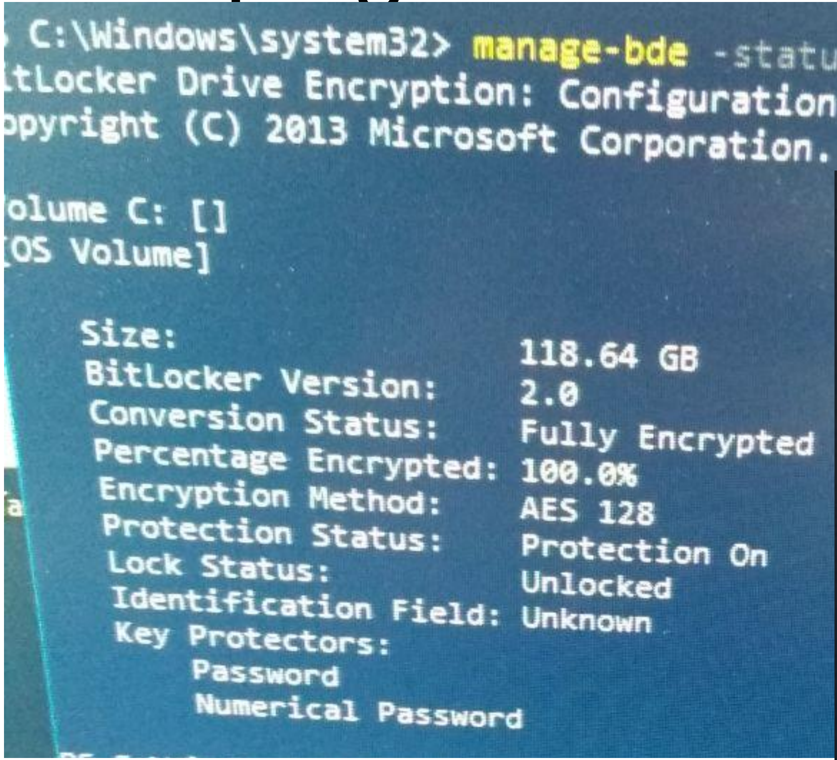


```
Fast Boot                                   Ultra Fast
SATA Support                                All Sata Devices
VGA Support                                 Auto
USB Support                                 Partial Initial
PS2 Devices Support                         Enabled
NetWork Stack Driver Support                Disabled
Next Boot After AC Power Loss               Fast Boot

Mouse Speed                                 1 X


Windows 8/10 Features                       Other OS
LAN PXE Boot Option ROM                     Disabled
Storage Boot Option Control                 Legacy
Other PCI devices                           Legacy
```

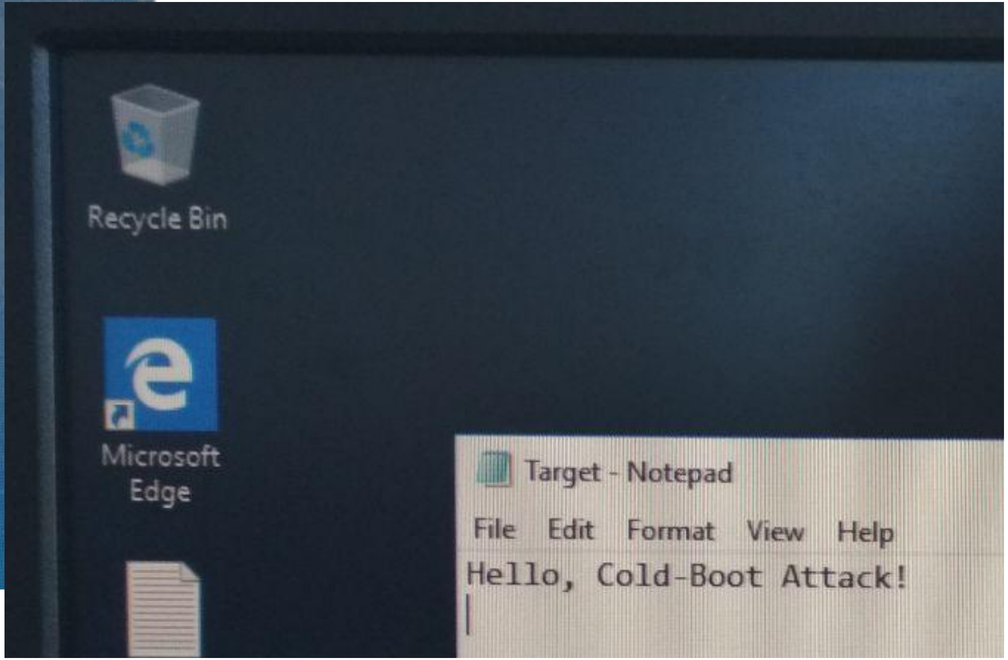
Dumping on ~~Bare~~ Brutal Metal



```
 C:\Windows\system32> manage-bde -status c:
tLocker Drive Encryption: Configuration Tool v
opyright (C) 2013 Microsoft Corporation. All ri

olume C: []
[OS Volume]

    Size:                     118.64 GB
    BitLocker Version:        2.0
    Conversion Status:        Fully Encrypted
    Percentage Encrypted:     100.0%
    Encryption Method:        AES 128
    Protection Status:        Protection On
    Lock Status:              Unlocked
    Identification Field:     Unknown
    Key Protectors:
        Password
        Numerical Password
```

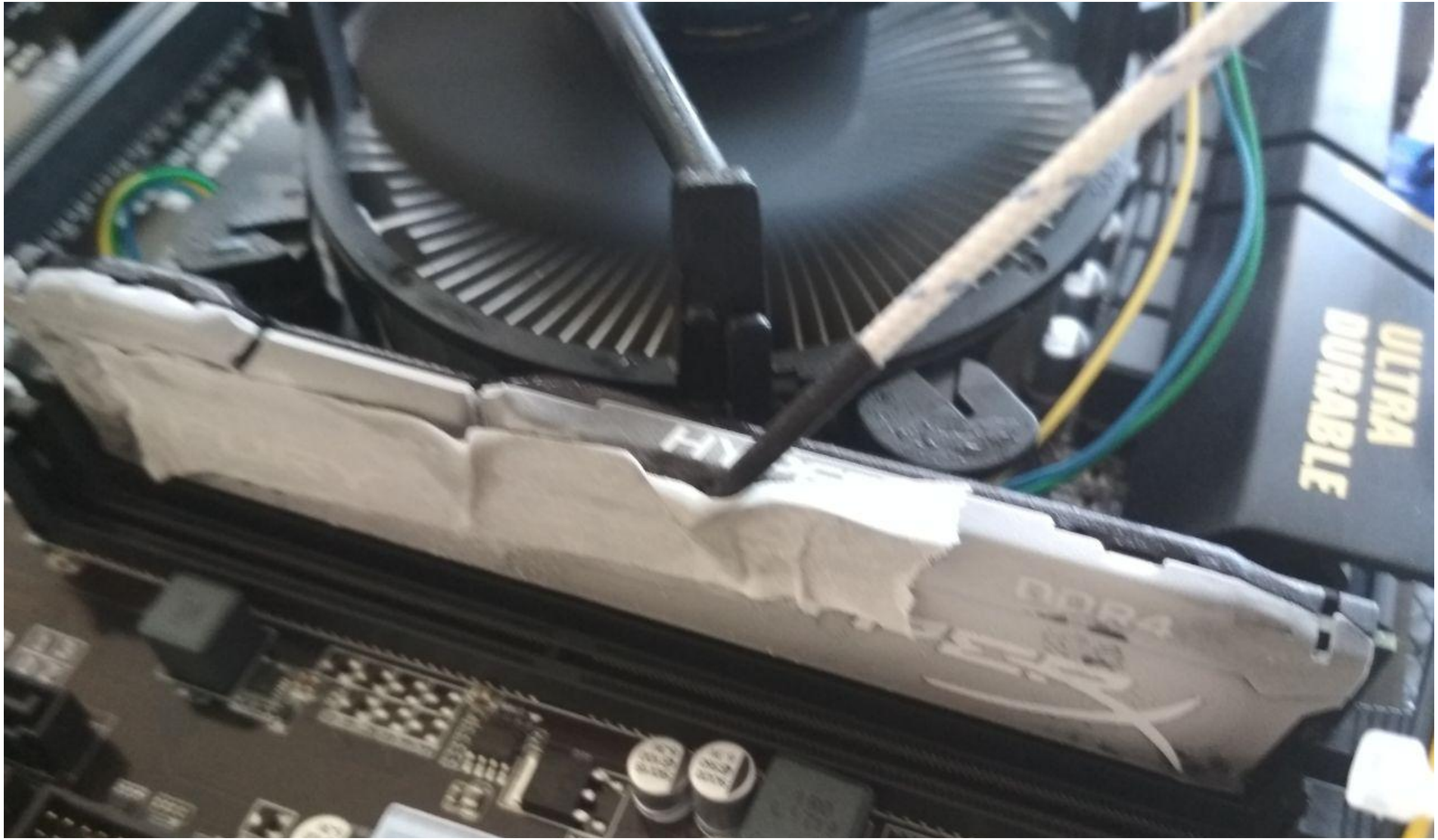


Hello, Cold-Boot Attack!

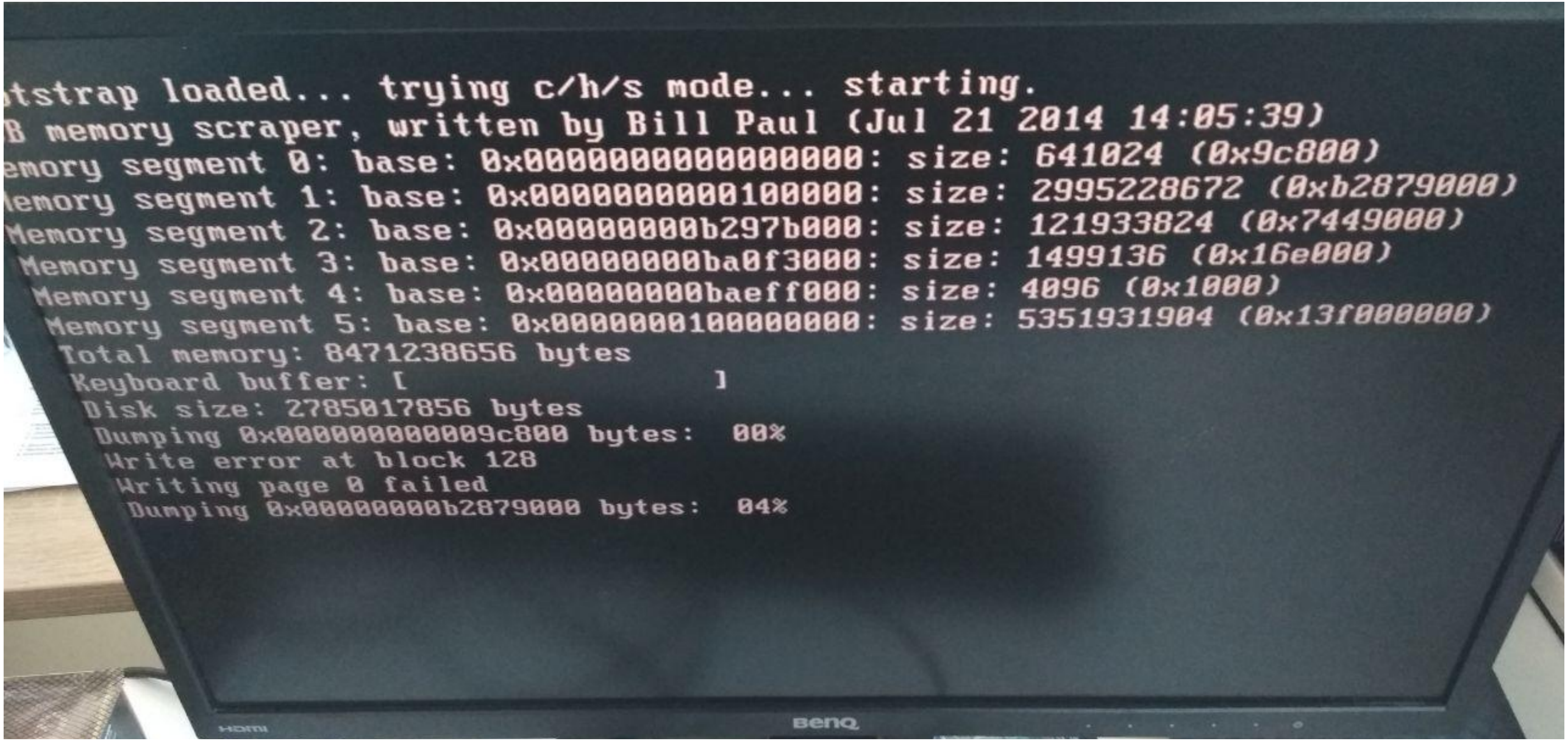
Dumping on ~~Bare~~ Brutal Metal

Dumping on ~~Bare~~ Brutal Metal

Dumping on ~~Bare~~ Brutal Metal

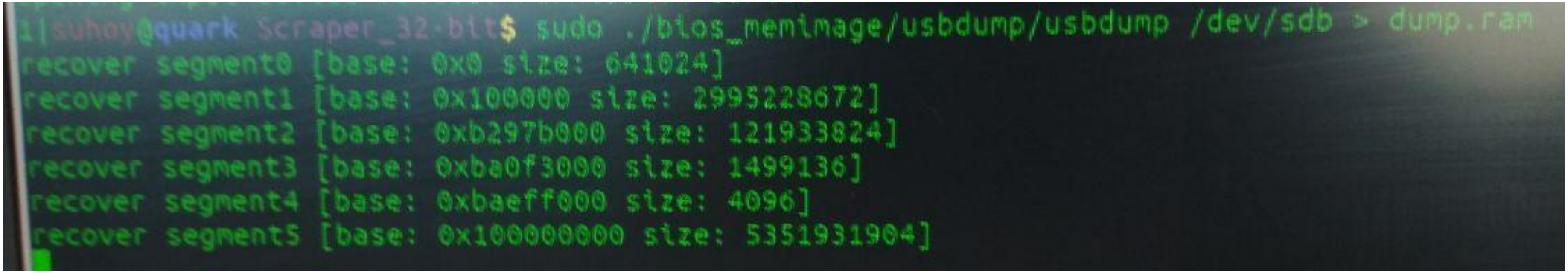


Dumping on ~~Bare~~ Brutal Metal



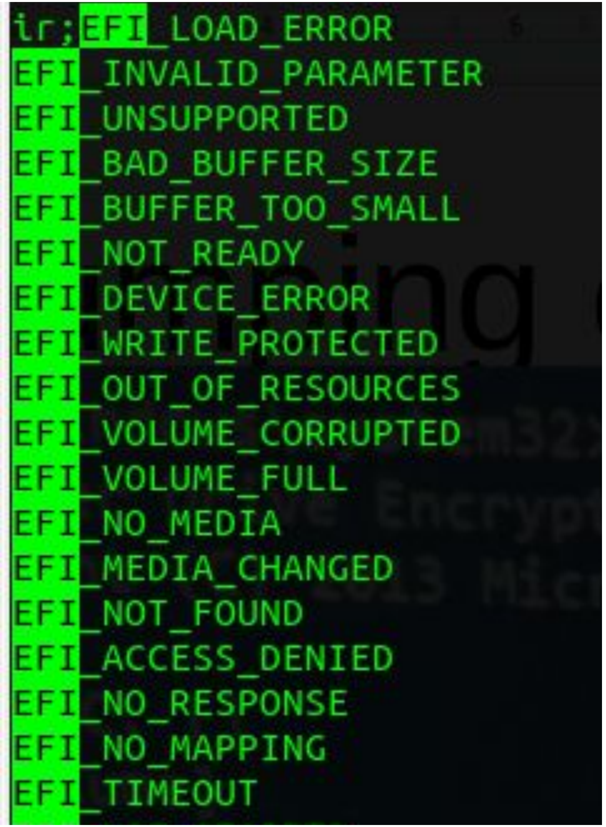
```
tstrap loaded... trying c/h/s mode... starting.
B memory scraper, written by Bill Paul (Jul 21 2014 14:05:39)
emory segment 0: base: 0x0000000000000000: size: 641024 (0x9c800)
lemory segment 1: base: 0x0000000000100000: size: 2995228672 (0xb2879000)
Memory segment 2: base: 0x00000000b297b000: size: 121933824 (0x7449000)
Memory segment 3: base: 0x00000000ba0f3000: size: 1499136 (0x16e000)
Memory segment 4: base: 0x00000000baeff000: size: 4096 (0x1000)
Memory segment 5: base: 0x0000000100000000: size: 5351931904 (0x13f000000)
Total memory: 8471238656 bytes
Keyboard buffer: [                    ]
Disk size: 2785017856 bytes
Dumping 0x000000000009c800 bytes:  00%
Write error at block 128
Writing page 0 failed
Dumping 0x00000000b2879000 bytes:  04%
```

Dumping on ~~Bare~~ Brutal Metal

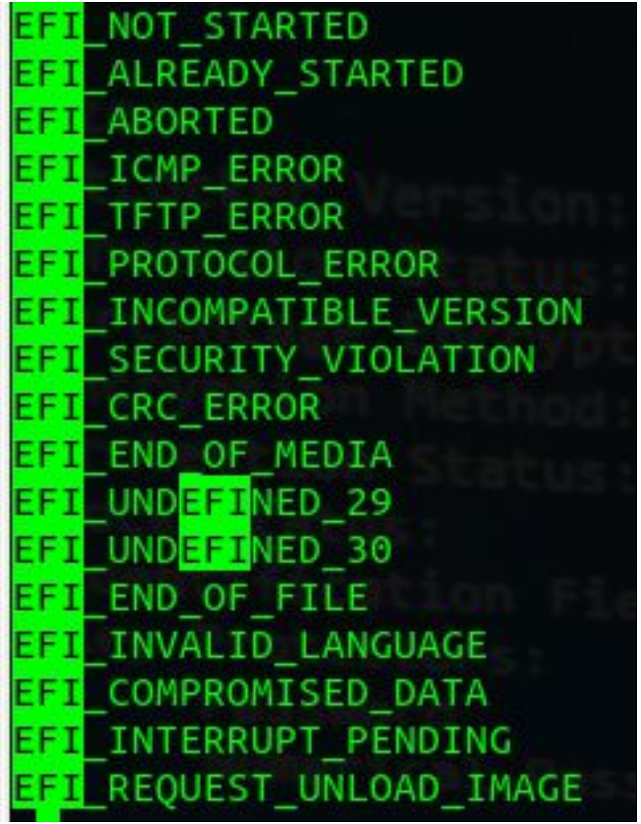


```
1|suhoy@quark Scraper_32-bit$ sudo ./bios_memimage/usbdump/usbdump /dev/sdb > dump.ram
recover segment0 [base: 0x0 size: 641024]
recover segment1 [base: 0x100000 size: 2995228672]
recover segment2 [base: 0xb297b000 size: 121933824]
recover segment3 [base: 0xba0f3000 size: 1499136]
recover segment4 [base: 0xbaeff000 size: 4096]
recover segment5 [base: 0x100000000 size: 5351931904]
```

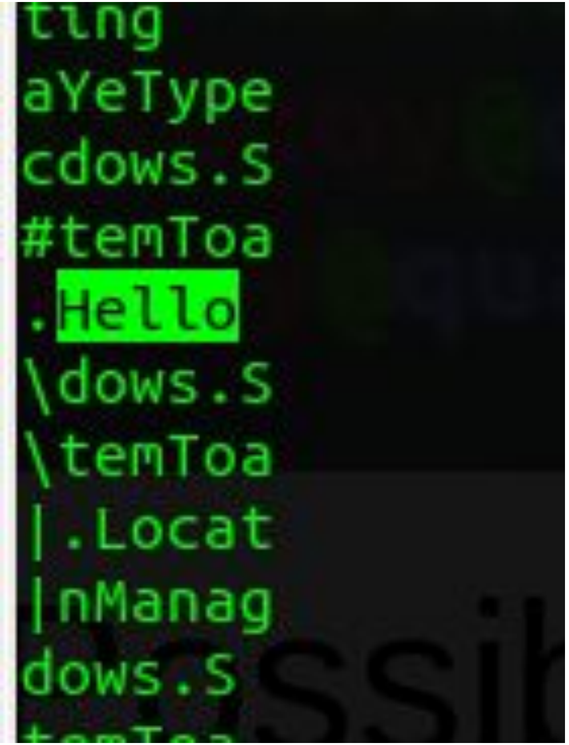
Dumping on ~~Bare~~ Brutal Metal



```
ir;EFI_LOAD_ERROR
EFI_INVALID_PARAMETER
EFI_UNSUPPORTED
EFI_BAD_BUFFER_SIZE
EFI_BUFFER_TOO_SMALL
EFI_NOT_READY
EFI_DEVICE_ERROR
EFI_WRITE_PROTECTED
EFI_OUT_OF_RESOURCES
EFI_VOLUME_CORRUPTED
EFI_VOLUME_FULL
EFI_NO_MEDIA
EFI_MEDIA_CHANGED
EFI_NOT_FOUND
EFI_ACCESS_DENIED
EFI_NO_RESPONSE
EFI_NO_MAPPING
EFI_TIMEOUT
```

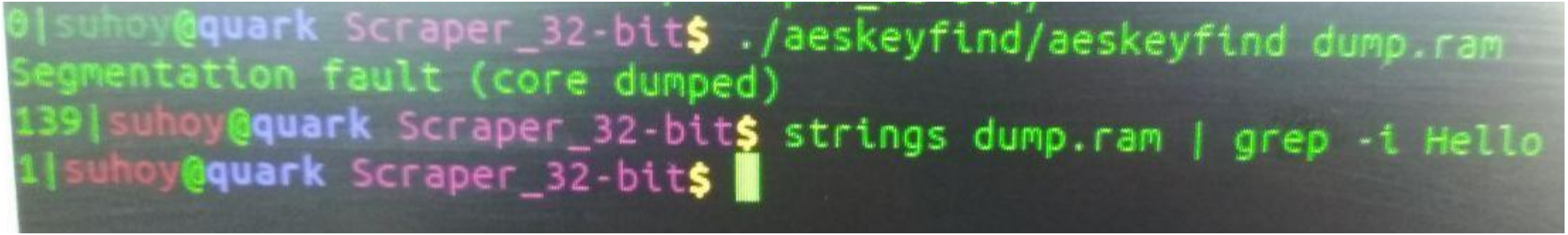


```
EFI_NOT_STARTED
EFI_ALREADY_STARTED
EFI_ABORTED
EFI_ICMP_ERROR
EFI_TFTP_ERROR
EFI_PROTOCOL_ERROR
EFI_INCOMPATIBLE_VERSION
EFI_SECURITY_VIOLATION
EFI_CRC_ERROR
EFI_END_OF_MEDIA
EFI_UNDEFINED_29
EFI_UNDEFINED_30
EFI_END_OF_FILE
EFI_INVALID_LANGUAGE
EFI_COMPROMISED_DATA
EFI_INTERRUPT_PENDING
EFI_REQUEST_UNLOAD_IMAGE
```



```
ting
aYeType
cdows.S
#temToa
.Hello
\dows.S
\temToa
|.Locat
|nManag
dows.S
```

Dumping on ~~Bare~~ Brutal Metal



```
0|suhoy@quark Scraper_32-bit$ ./aeskeyfind/aeskeyfind dump.ram
Segmentation fault (core dumped)
139|suhoy@quark Scraper_32-bit$ strings dump.ram | grep -i Hello
1|suhoy@quark Scraper_32-bit$
```

Possible reasons:

- More than 4 GiB
- Do not believe in binaries from Internet
- Bad BIOS / hardware
- DDR4 degrades too fast

Dumping on ~~Bare~~ Brutal Metal

Stay tuned?

Back to theory ...

Related Works, Standards and Resources

1. Memory Forensics over the IEEE 1394 Interface, Witherden (2010), pdf
2. The Chilling Reality of Cold Boot Attacks(2018),F-Secure lab, blog, youtube
3. Demo is shown in InfoSec (2019), (September 2014 ??)
4. DDR DIMM SPD Adapter for Raspberry Pi, Illya T. (2014-2018), xDevs.com

Related Works, Standards and Resources

1. Memory Forensics over the IEEE 1394 Interface, Witherden (2010), pdf
2. The Chilling Reality of Cold Boot Attacks(2018),F-Secure lab, blog, youtube
3. Demo is shown in InfoSec (2019), (September 2014 ??)
4. DDR DIMM SPD Adapter for Raspberry Pi, Illya T. (2014-2018), xDevs.com
    a. **HX424C15FB2K2/16**, Kingston Memory Module Specification, pdf
    b. HyperX Fury DDR4 RAM, Web-page
    c. HyperX Part Number Decoder, Web-page
    d. **DDR4 SDRAM Standard - Jedec, $284,** download page
    e. DDR4 SDRAM UDIMM Design Specification, Revision 1.10, 44p.

Related Works, Standards and Resources

1. Memory Forensics over the IEEE 1394 Interface, Witherden (2010), pdf
2. The Chilling Reality of Cold Boot Attacks(2018),F-Secure lab, blog, youtube
3. Demo is shown in InfoSec (2019), (September 2014 ??)
4. DDR DIMM SPD Adapter for Raspberry Pi, Illya T. (2014-2018), xDevs.com
    a. **HX424C15FB2K2/16**, Kingston Memory Module Specification, pdf
    b. HyperX Fury DDR4 RAM, Web-page
    c. HyperX Part Number Decoder, Web-page
    d. DDR4 SDRAM Standard - Jedec, $284, download page
    e. DDR4 SDRAM UDIMM Design Specification, Revision 1.10, 44p.
5. OSDev.org - *the longest way*
6. wikipedia.org - *good start to explore about PC components*
7. A lot of similar videos and materials ...

Related Works, Standards and Resources

1. Memory Forensics over the IEEE 1394 Interface, Witherden (2010), pdf
2. The Chilling Reality of Cold Boot Attacks(2018),F-Secure lab, blog, youtube
3. Demo is shown in InfoSec (2019), (September 2014 ??)
4. DDR DIMM SPD Adapter for Raspberry Pi, Illya T. (2014-2018), xDevs.com
    a. **HX424C15FB2K2/16**, Kingston Memory Module Specification, pdf
    b. HyperX Fury DDR4 RAM, Web-page
    c. HyperX Part Number Decoder, Web-page
    d. DDR4 SDRAM Standard - Jedec, $284, download page
    e. DDR4 SDRAM UDIMM Design Specification, Revision 1.10, 44p.
5. OSDev.org - *the longest way*
6. wikipedia.org - *general PC structure*
7. A lot of similar videos and materials ...

Before we start….

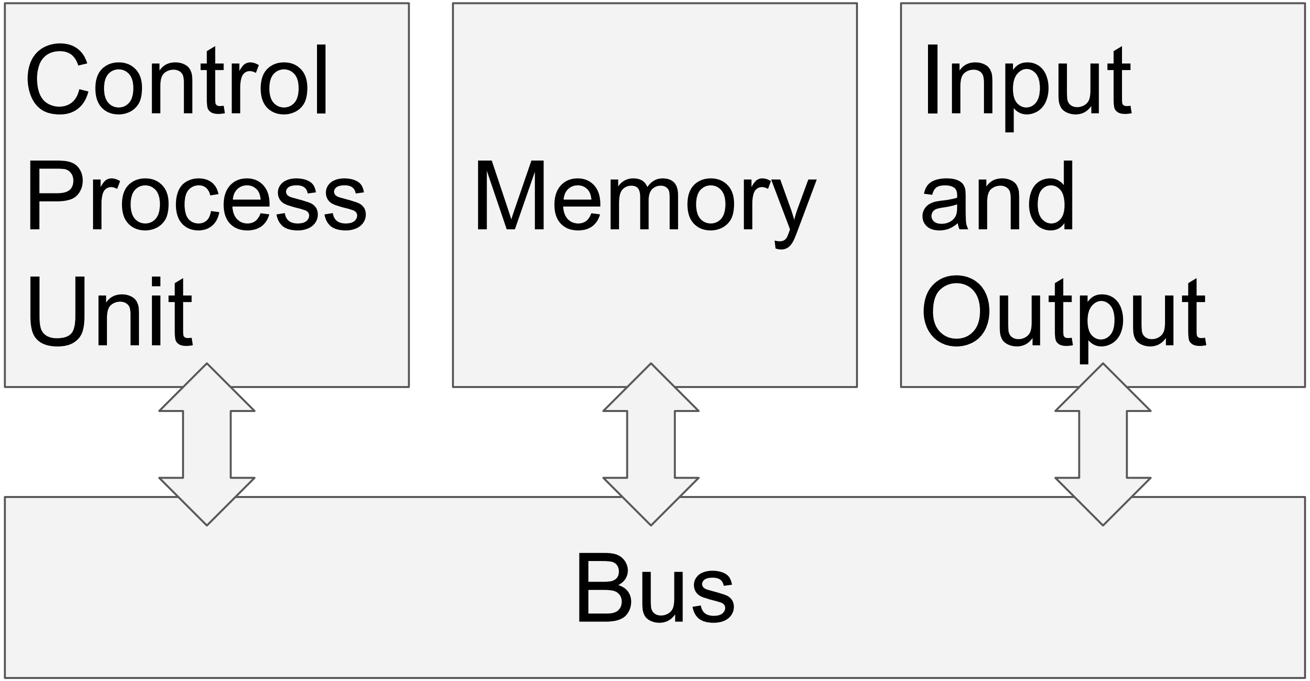
Broad our task

How to dump RAM?

↓

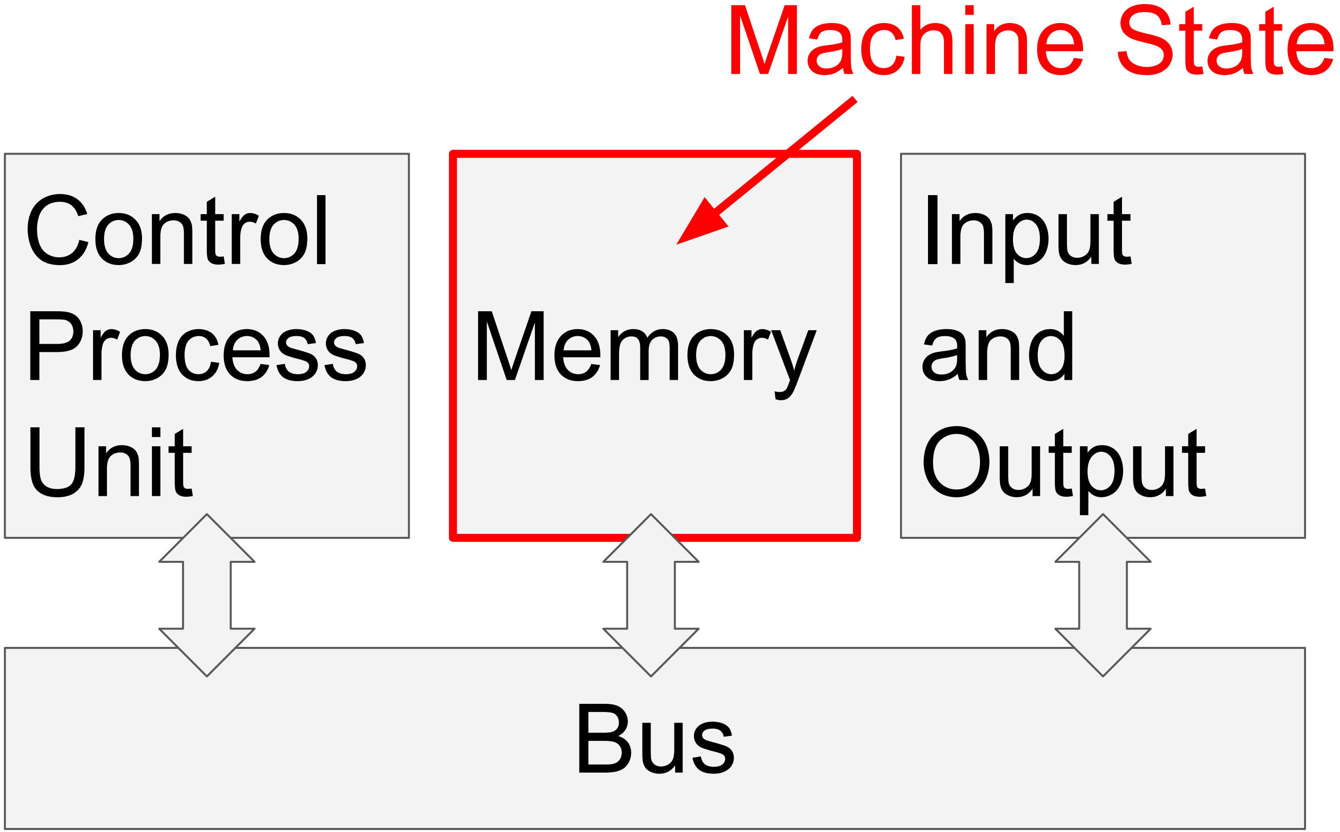
How to extract Machine State?

What is Machine State?



https://en.wikipedia.org/wiki/Von_Neumann_architecture

What is Machine State?



Machine State

Control Process Unit

Memory

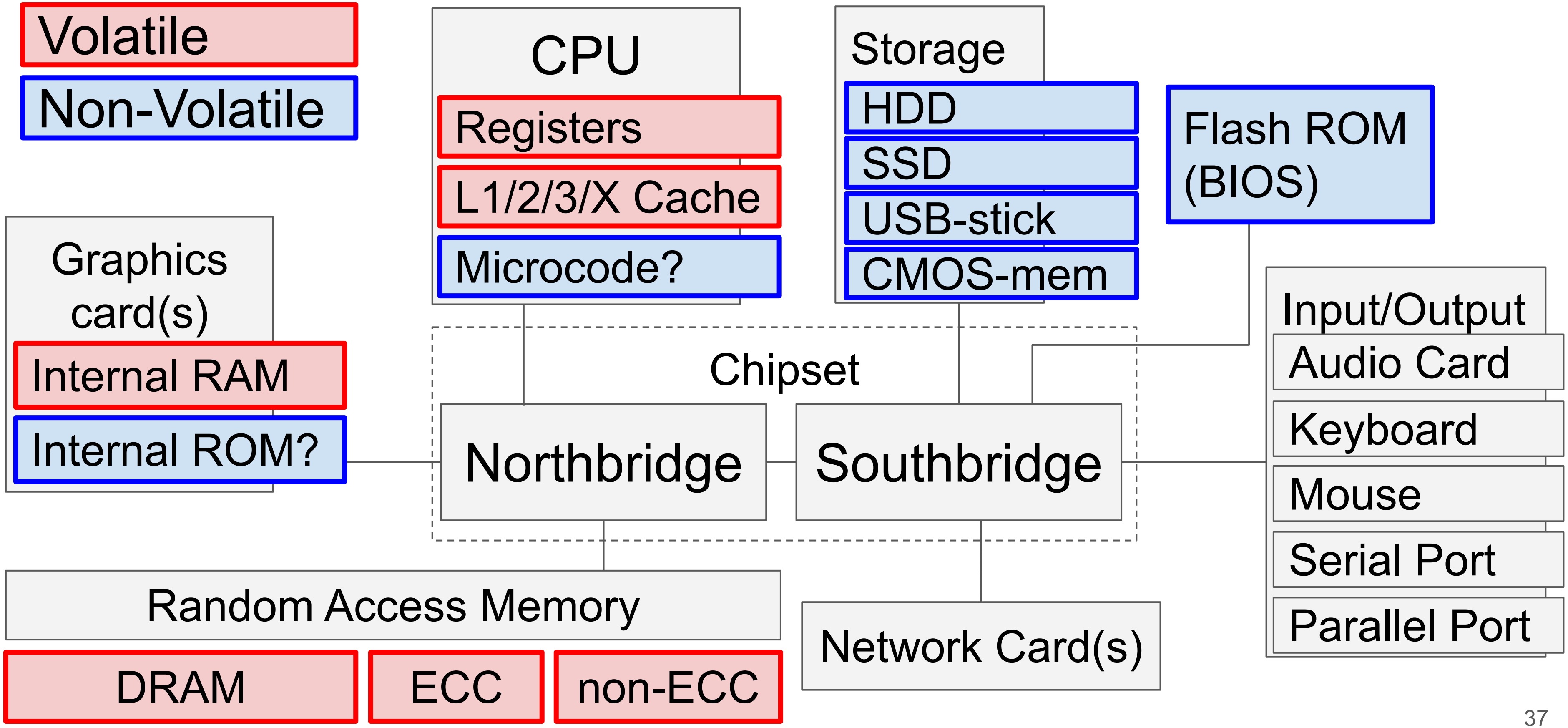
Input and Output

Bus

https://en.wikipedia.org/wiki/Von_Neumann_architecture

Simple, but…

What is Machine State?



Volatile

Non-Volatile

CPU

Registers

L1/2/3/X Cache

Microcode?

Storage

HDD

SSD

USB-stick

CMOS-mem

Flash ROM (BIOS)

Graphics card(s)

Internal RAM

Internal ROM?

Chipset

Northbridge

Southbridge

Input/Output

Audio Card

Keyboard

Mouse

Serial Port

Parallel Port

Random Access Memory

DRAM

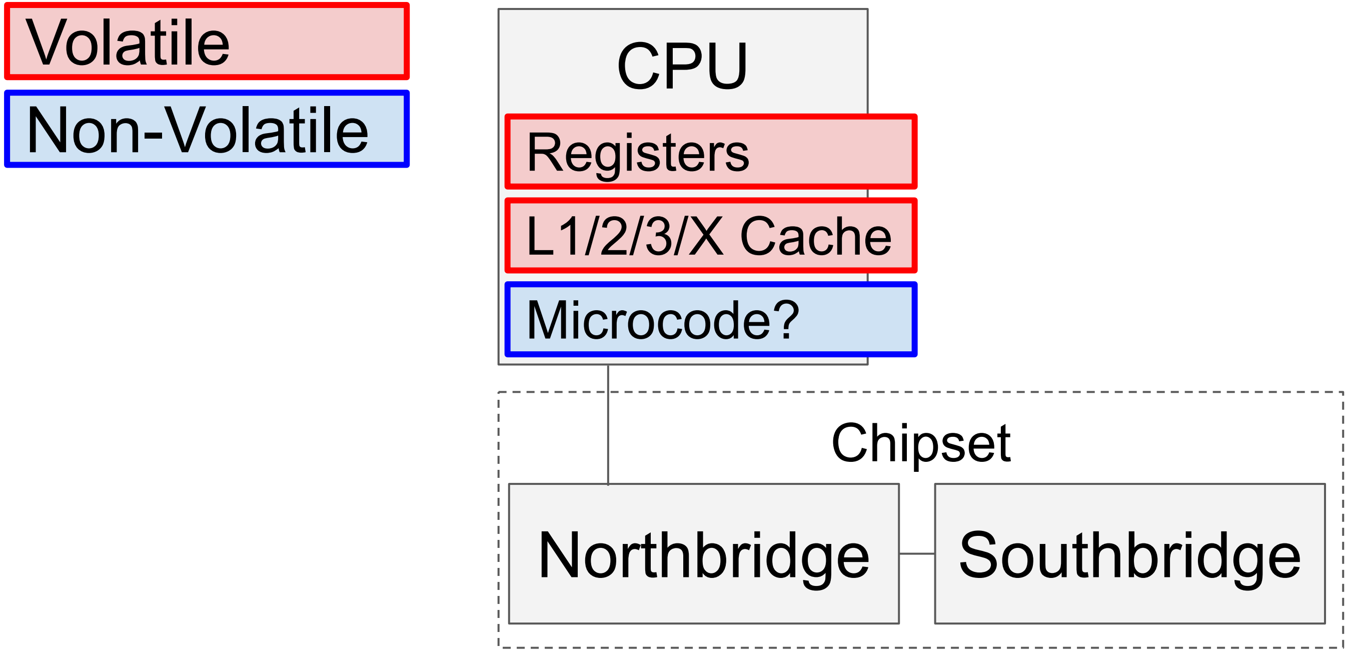
ECC

non-ECC

Network Card(s)

Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

What is Machine State?



Volatile

Non-Volatile

CPU

Registers

L1/2/3/X Cache

Microcode?

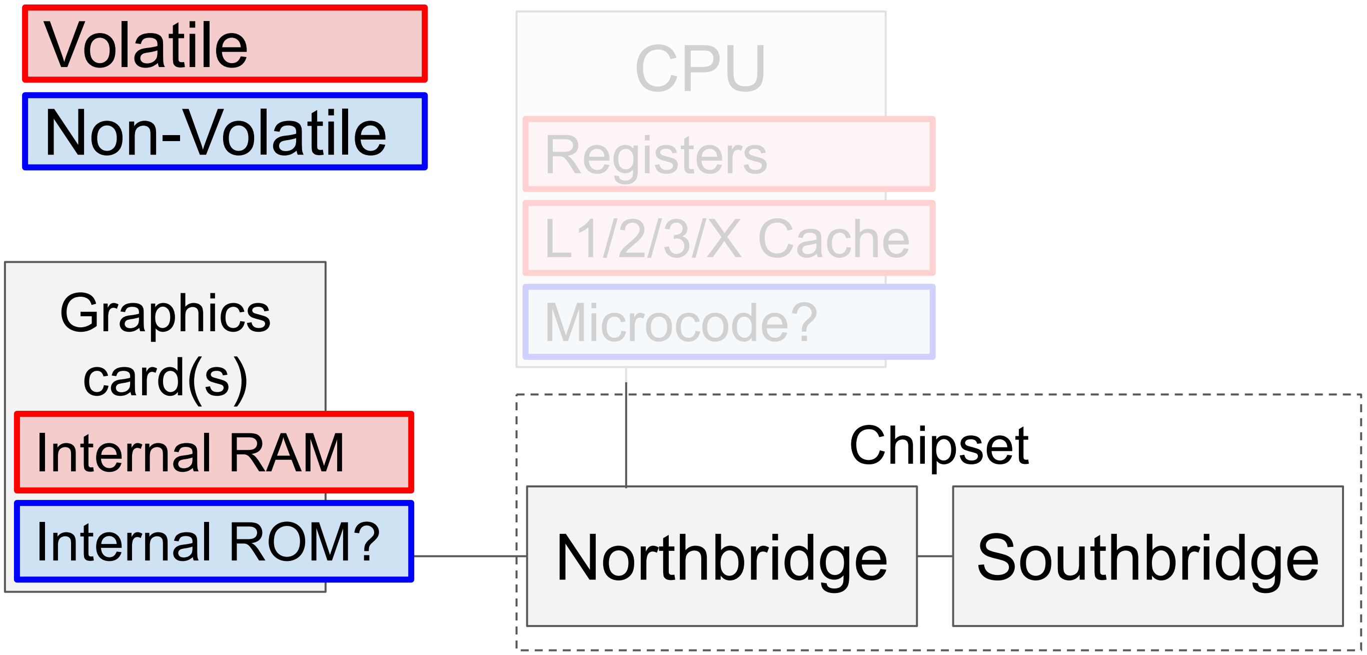
Chipset

Northbridge

Southbridge

Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

What is Machine State?



Volatile

Non-Volatile

CPU

Registers

L1/2/3/X Cache

Microcode?

Graphics card(s)

Internal RAM

Internal ROM?

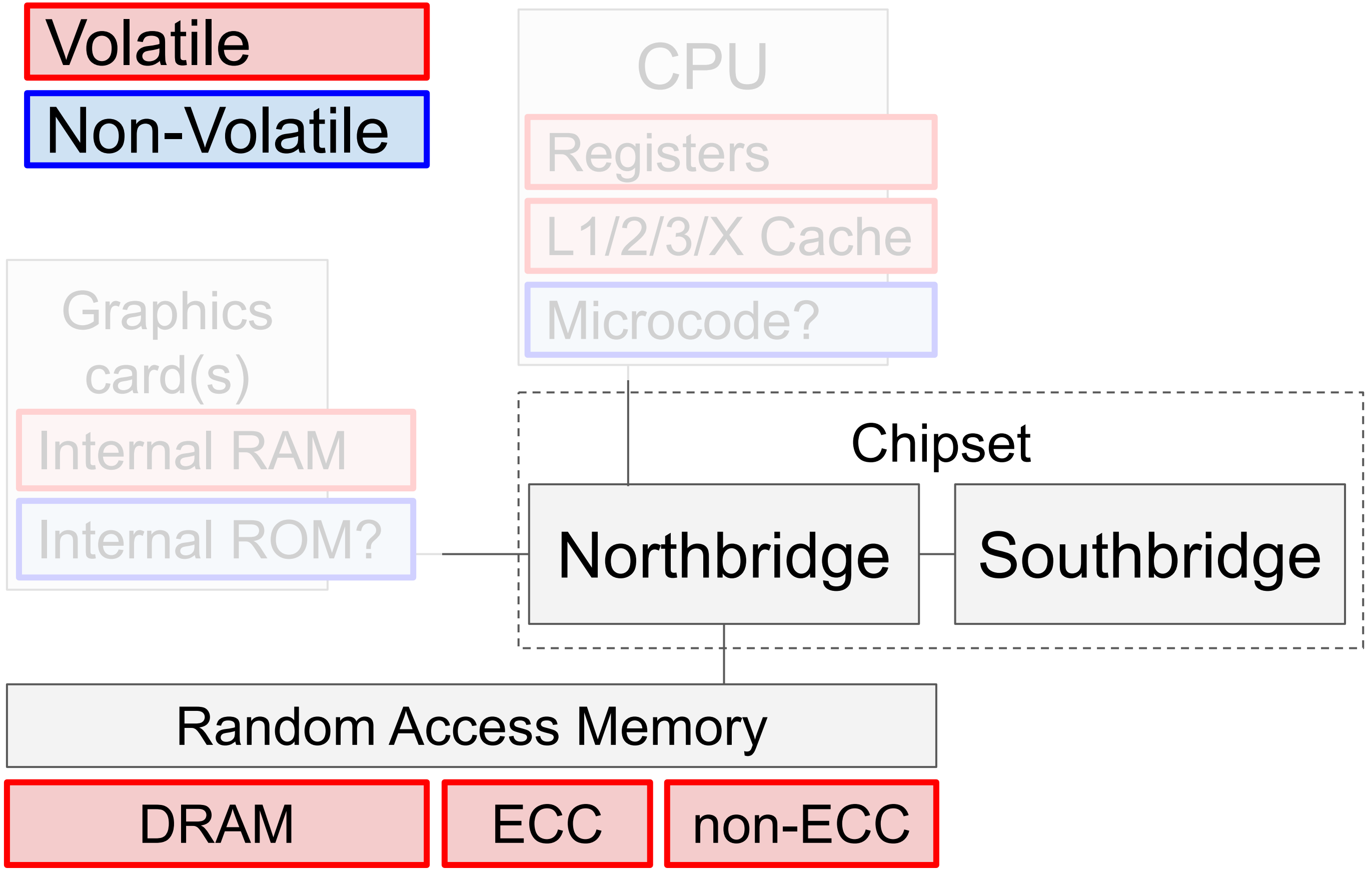
Chipset

Northbridge

Southbridge

Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

What is Machine State?



Volatile

Non-Volatile

CPU

Registers

L1/2/3/X Cache

Microcode?

Graphics card(s)

Internal RAM

Internal ROM?

Chipset

Northbridge

Southbridge

Random Access Memory

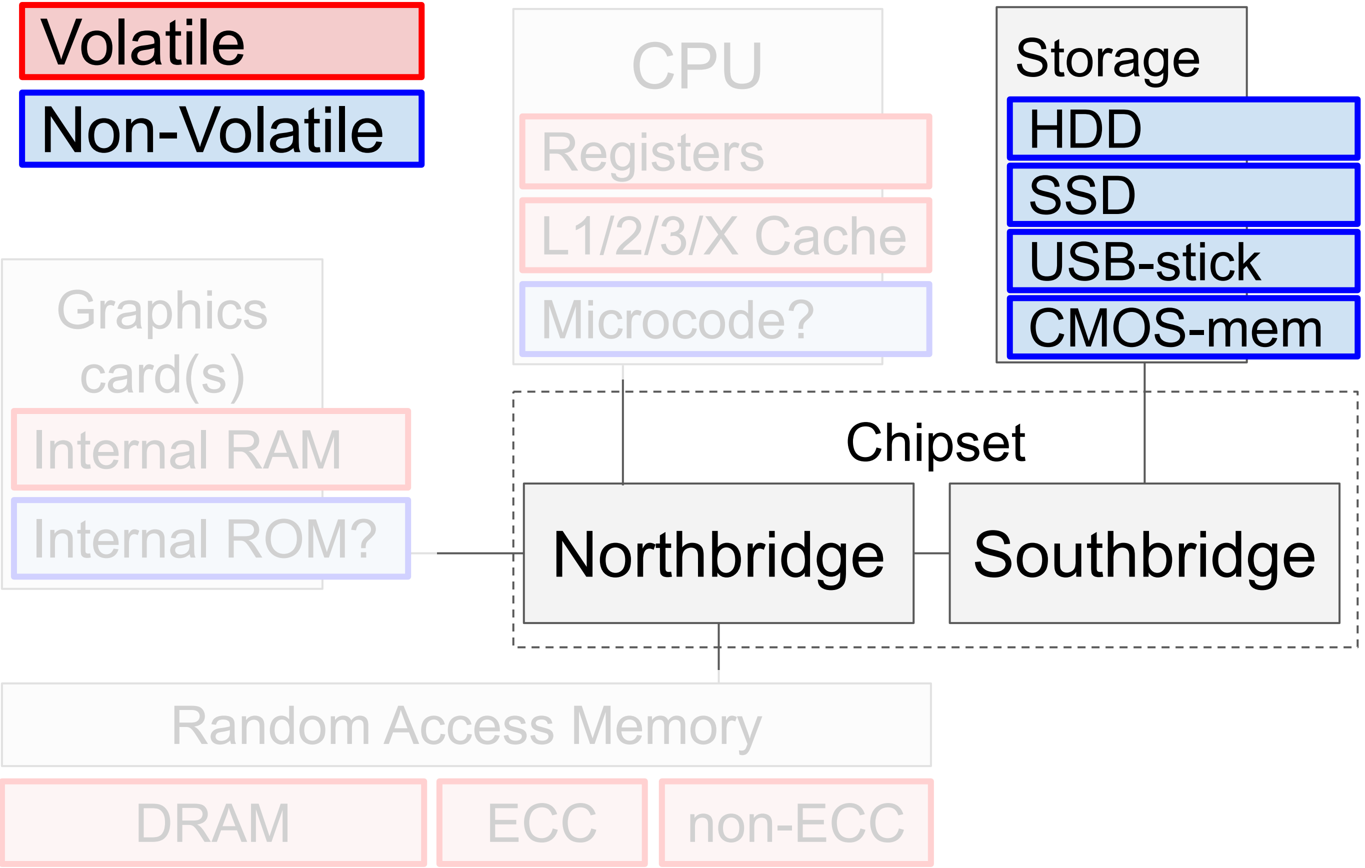
DRAM

ECC

non-ECC

Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

What is Machine State?



Volatile

Non-Volatile

CPU

Registers

L1/2/3/X Cache

Microcode?

Storage

HDD

SSD

USB-stick

CMOS-mem

Graphics card(s)

Internal RAM

Internal ROM?

Chipset

Northbridge

Southbridge

Random Access Memory

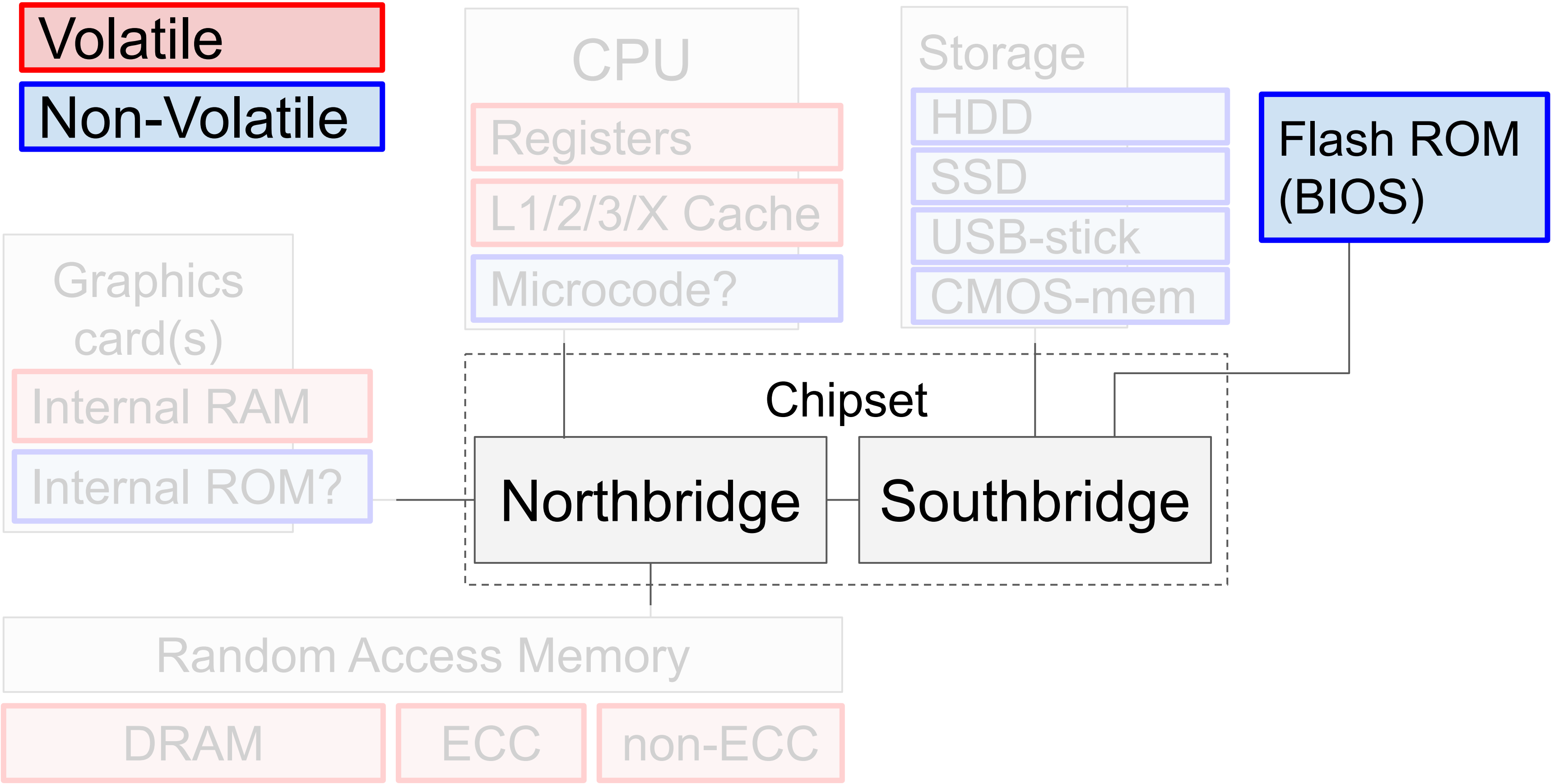
DRAM

ECC

non-ECC

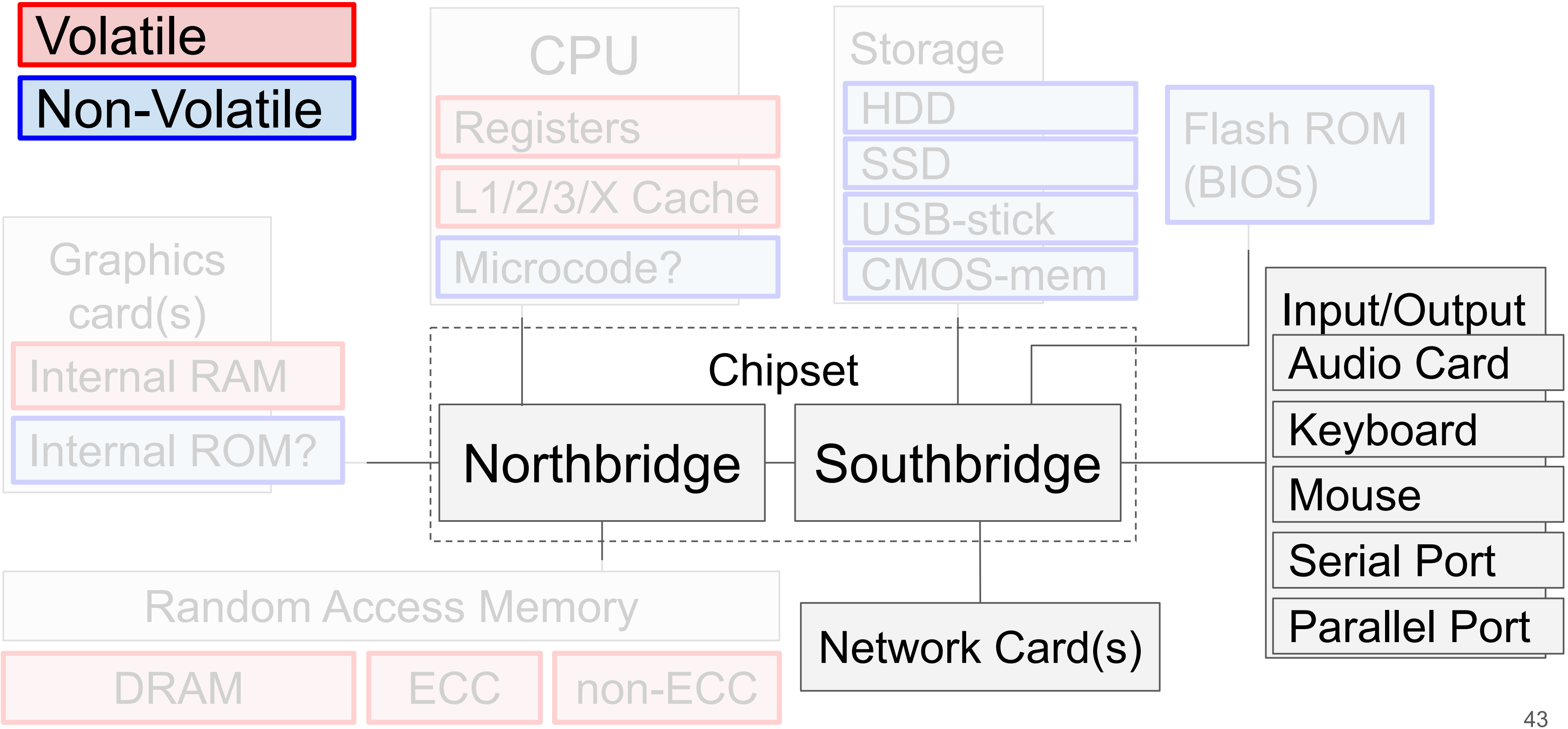
Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

What is Machine State?



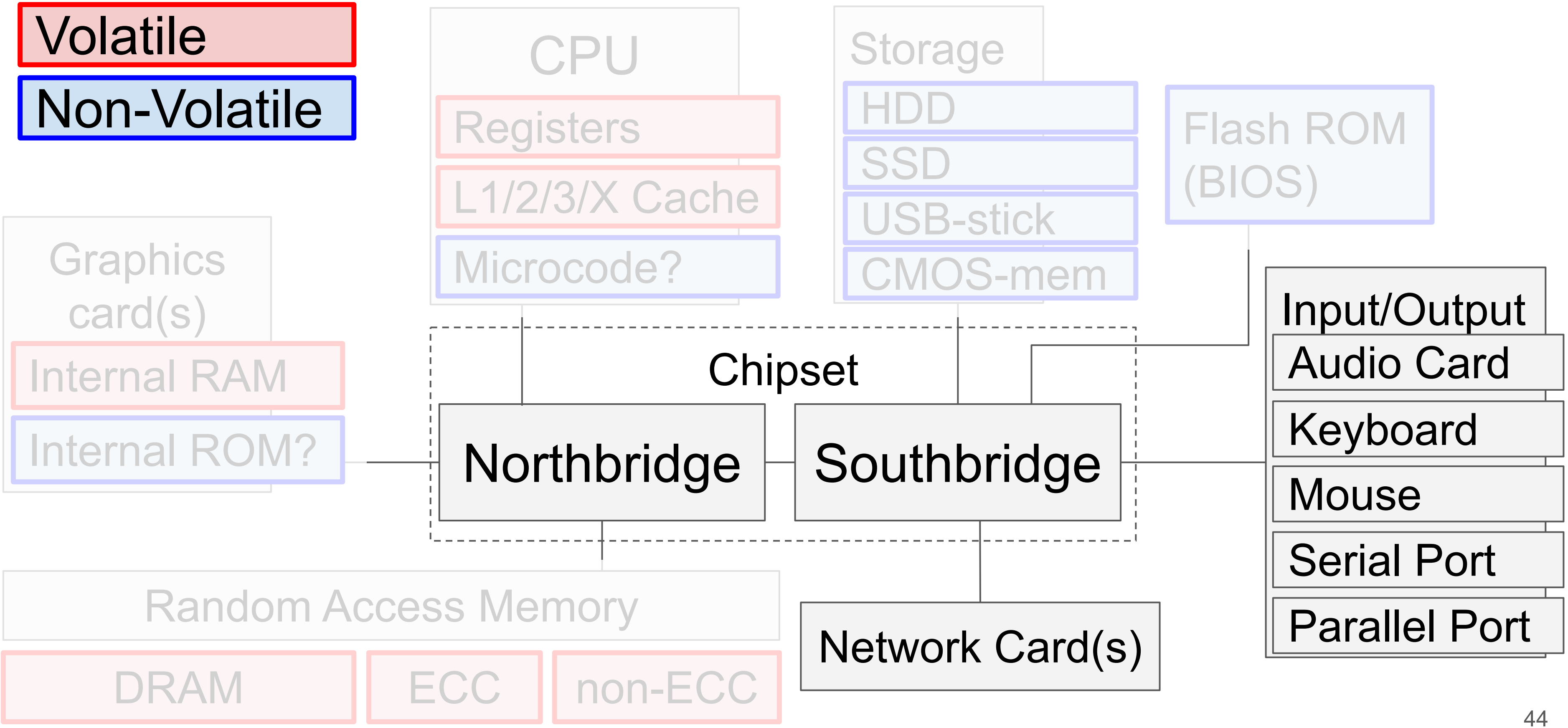
Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

What is Machine State?



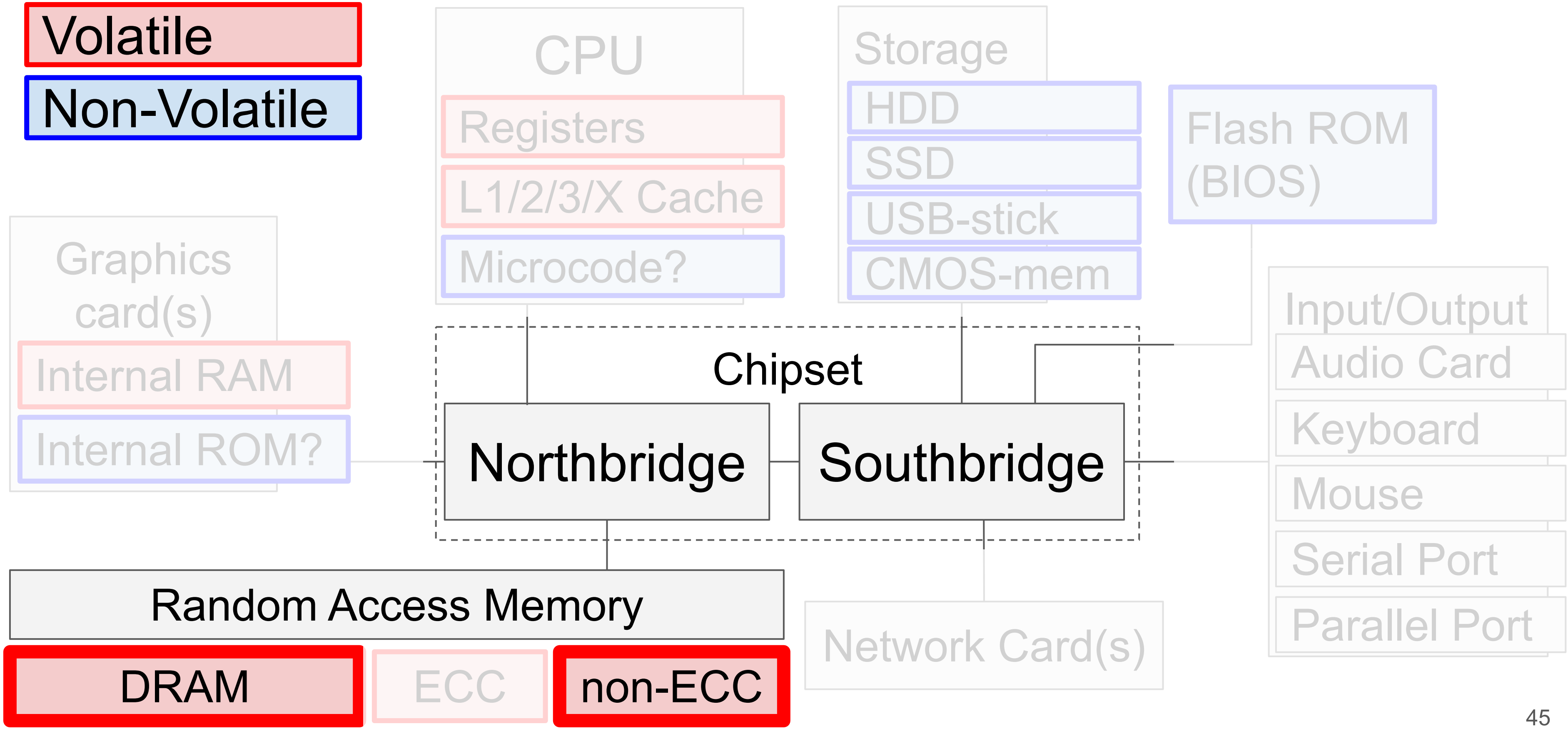
Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

Question: Is I/O really *stateless*?



Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

Defining the objective...



Volatile

Non-Volatile

CPU

Registers

L1/2/3/X Cache

Microcode?

Storage

HDD

SSD

USB-stick

CMOS-mem

Flash ROM (BIOS)

Graphics card(s)

Internal RAM

Internal ROM?

Chipset

Northbridge

Southbridge

Input/Output

Audio Card

Keyboard

Mouse

Serial Port

Parallel Port

Random Access Memory

DRAM

ECC

non-ECC

Network Card(s)

Inspired By: https://en.wikipedia.org/wiki/Motherboard#/media/File:Motherboard_diagram.svg

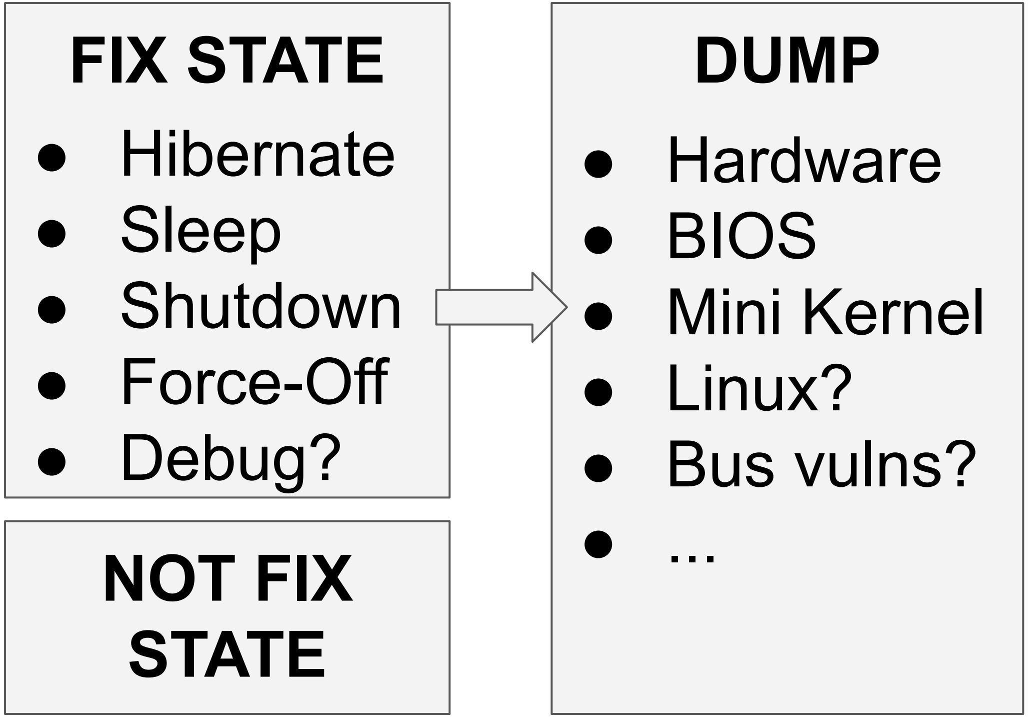
Extraction Procedure

FIX STATE

- Hibernate
- Sleep
- Shutdown
- Force-Off
- Debug?

NOT FIX STATE

Extraction Procedure



FIX STATE

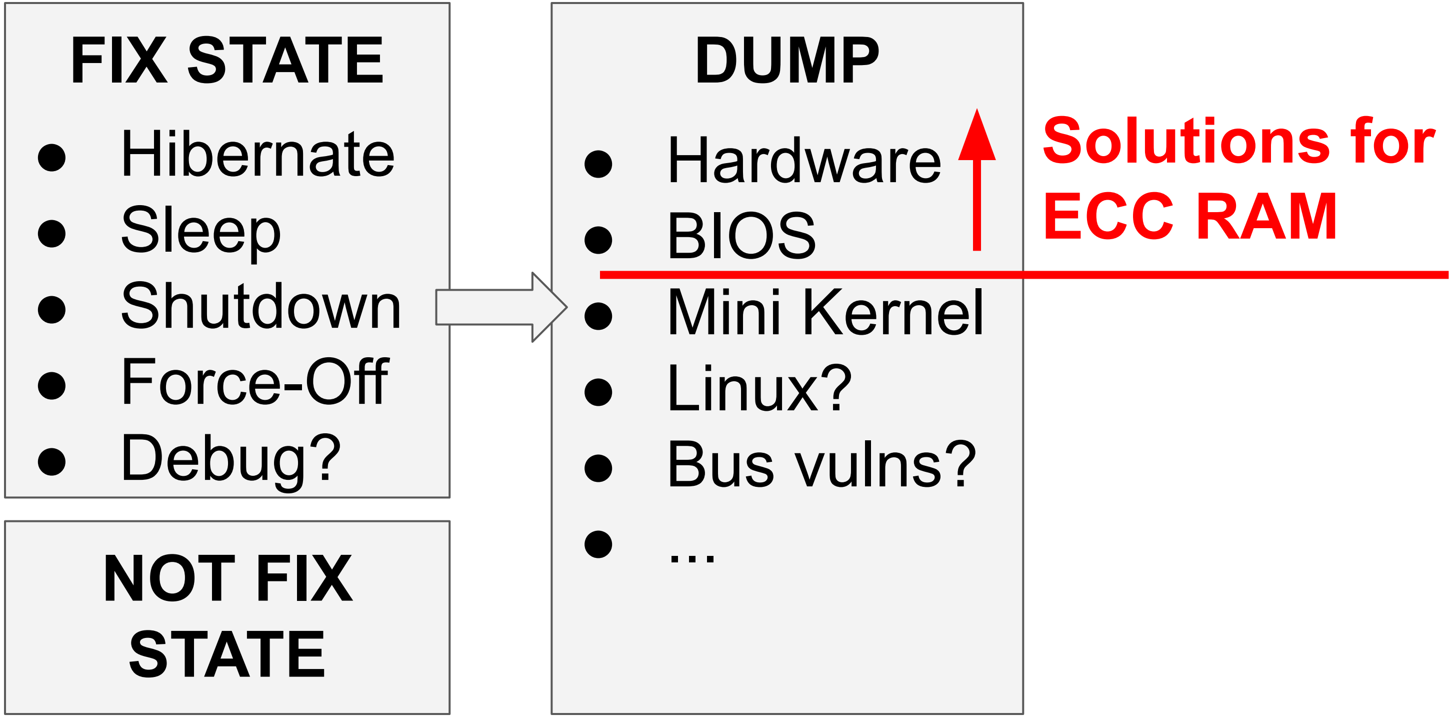
- Hibernate
- Sleep
- Shutdown
- Force-Off
- Debug?

NOT FIX STATE

DUMP

- Hardware
- BIOS
- Mini Kernel
- Linux?
- Bus vulns?
- ...

Extraction Procedure



FIX STATE

- Hibernate
- Sleep
- Shutdown
- Force-Off
- Debug?

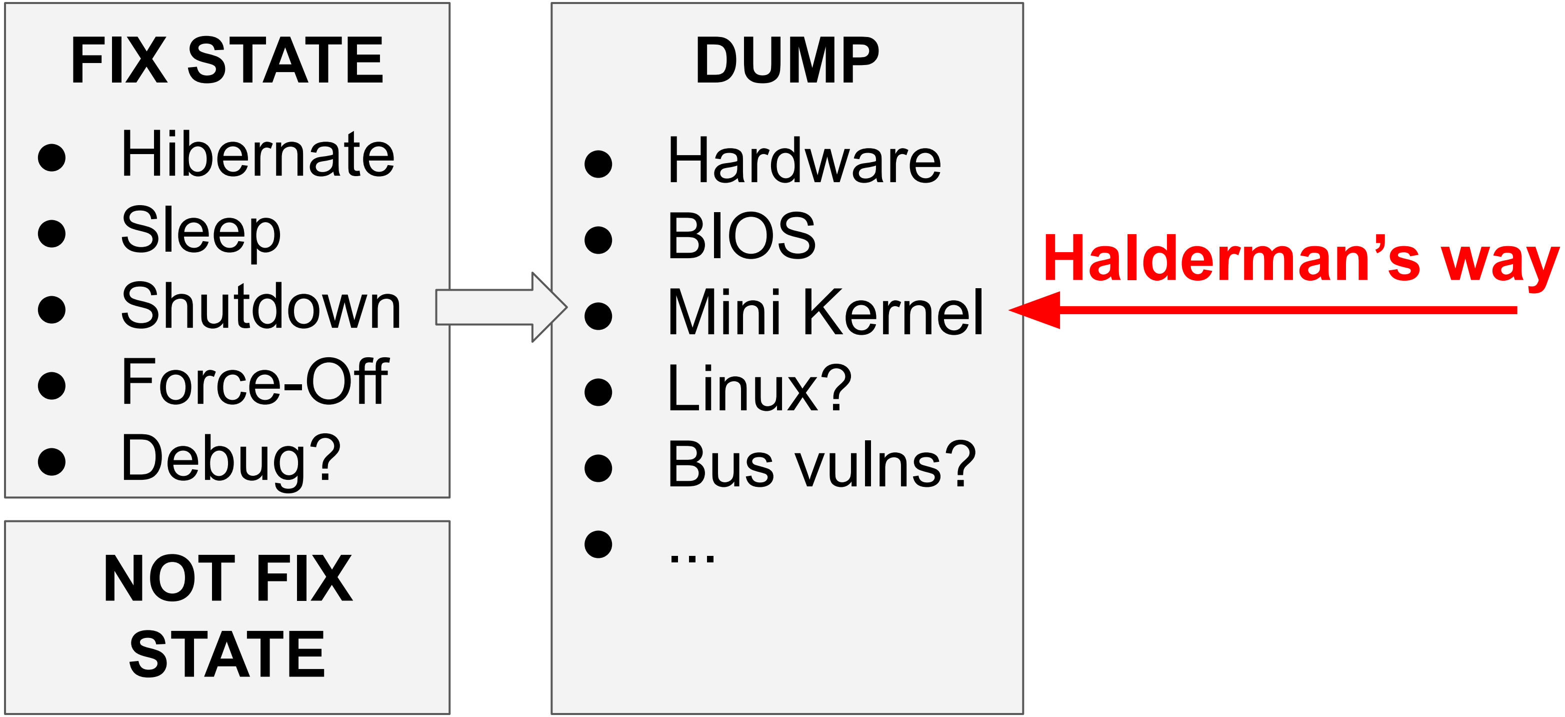
NOT FIX STATE

DUMP

- Hardware
- BIOS
- Mini Kernel
- Linux?
- Bus vulns?
- ...

Solutions for ECC RAM

Extraction Procedure



FIX STATE

- Hibernate
- Sleep
- Shutdown
- Force-Off
- Debug?

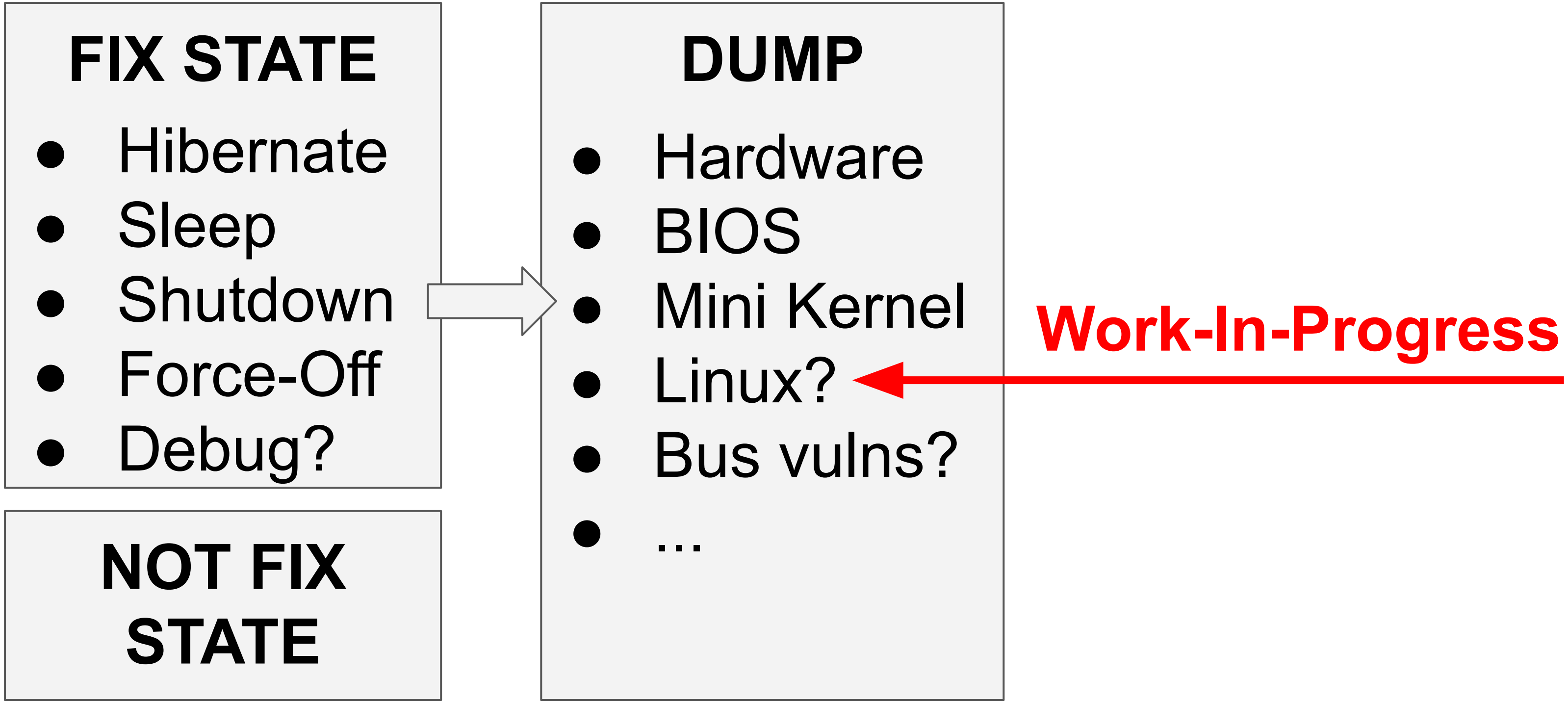
NOT FIX STATE

DUMP

- Hardware
- BIOS
- Mini Kernel
- Linux?
- Bus vulns?
- ...

Halderman's way

Extraction Procedure



FIX STATE

- Hibernate
- Sleep
- Shutdown
- Force-Off
- Debug?

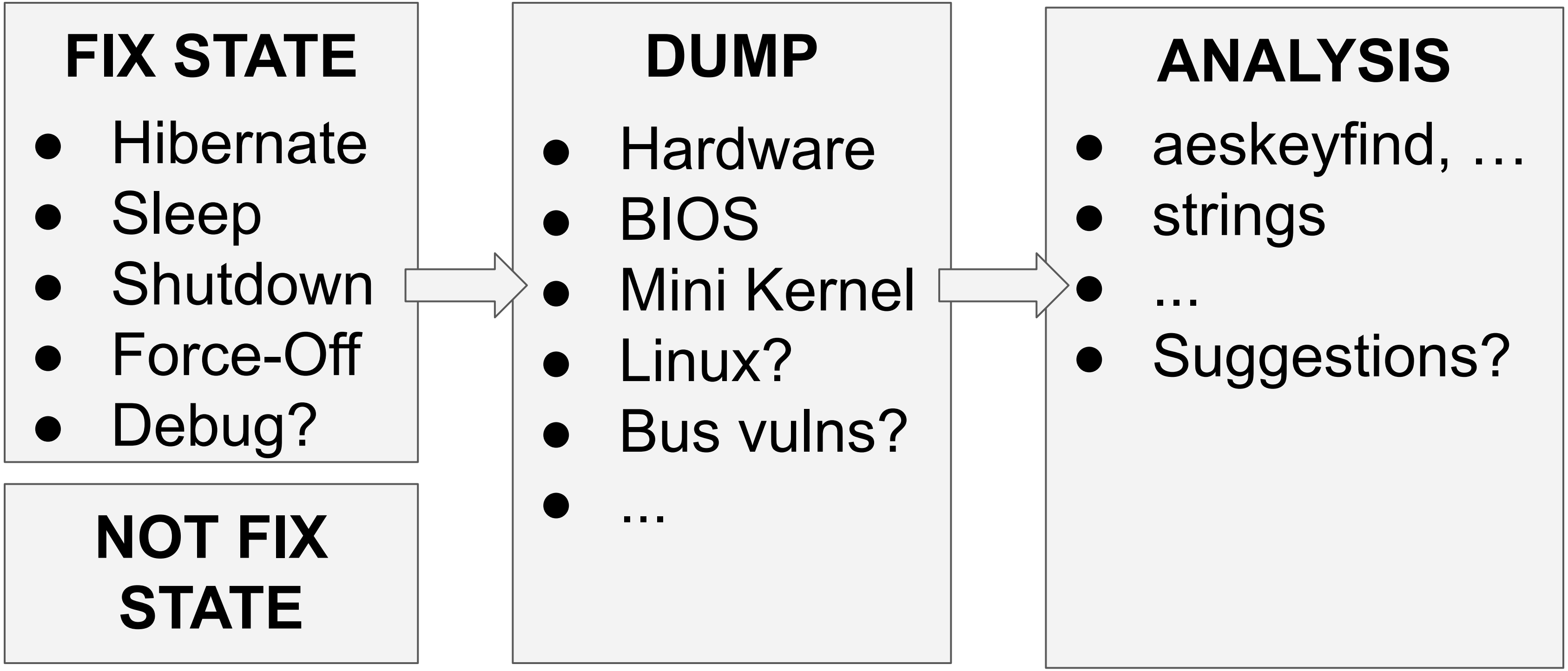
NOT FIX STATE

DUMP

- Hardware
- BIOS
- Mini Kernel
- Linux?
- Bus vulns?
- ...

Work-In-Progress

Extraction Procedure



FIX STATE

- Hibernate
- Sleep
- Shutdown
- Force-Off
- Debug?

NOT FIX STATE

DUMP

- Hardware
- BIOS
- Mini Kernel
- Linux?
- Bus vulns?
- ...

ANALYSIS

- aeskeyfind, …
- strings
- ...
- Suggestions?

Properties:

- Dump Consistency
- Dumping/Acquisition Speed
- Anti-dumping methods Availability
- Method interference (Impact on RAM Content)
- ...

FIX STATE

	Hibernate	Sleep	Shutdown	Force-Off
Consistency	Virtualization seems possible		OS Leftovers	Uncontrolled CPU state
Anti-dumping	YES	YES	YES	More Difficult

DUMP

	Hardware	**BIOS**	**Mini Kernel**	**Linux (Any OS)**
Method interference	~0	Few KiB	Few KiB-MiB	The Most Harmful

DUMP

Acquisition Speed depends on

- RAM volume
- using buses and devices

    i.e. USB, SATA, Ethernet, etc...

50 DUMP shades

HARDWARE REQUIRED BARRIER

50 DUMP shades

- Hardware
  - Raspberry Pi + DDR Connector? (as xDevs.com)
  - FPGA Devices (Like NanoBoard 3000) **[EXPENSIVE ~1k$]**
  - Open-Source Hardware (Respects Your Freedom)

HARDWARE REQUIRED BARRIER

50 DUMP shades

- Hardware
  - Raspberry Pi + DDR Connector? (as xDevs.com)
  - FPGA Devices (Like NanoBoard 3000) **[EXPENSIVE ~1k$]**
  - Open-Source Hardware (Respects Your Freedom)
- BIOS **[Experience WANTED]**
  - Coreboot (https://www.coreboot.org/)
  - u-boot (https://www.denx.de/wiki/U-Boot)

HARDWARE REQUIRED BARRIER

50 DUMP shades

- Hardware
  - Raspberry Pi + DDR Connector? (as xDevs.com)
  - FPGA Devices (Like NanoBoard 3000) **[EXPENSIVE ~1k$]**
  - Open-Source Hardware (Respects Your Freedom)
- BIOS **[Experience WANTED]**
  - Coreboot (https://www.coreboot.org/)
  - u-boot (https://www.denx.de/wiki/U-Boot)

HARDWARE REQUIRED BARRIER

- Mini Kernel - Following By Halderman Steps **[That x86]**
- Custom Linux - *Work In Progress*

Thank you for attention.
Any questions?

Ilya Sukhoplyuev

Innopolis SNE Student

i.sukhoplyuev@innopolis.university

Telegram: @suhoy95

Presentation: https://bit.ly/2waVeX1