Forensics, Malware and Penetration Testing

Memory forensics

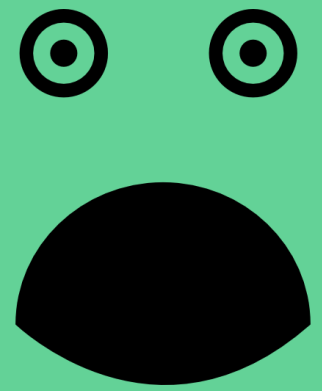
David Oswald and Andreea Radu

University of Birmingham

d.f.oswald@bham.ac.uk

Everything you always wanted to know about RAM*

(*but were afraid to ask)



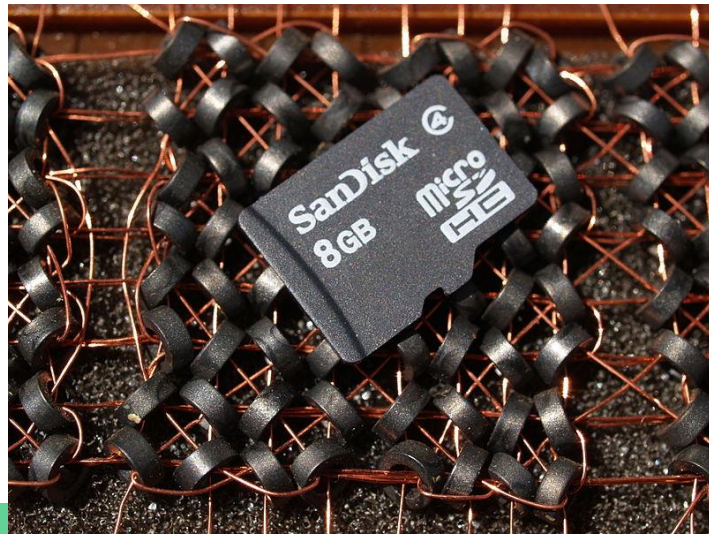
Outline

1. Disk forensics* ✓
2. Log file forensics ✓
3. Network forensics ✓
4. Memory forensics ←
5. Mobile devices (Android)

* May need RAM forensics, e.g., in case of full-disk encryption

Memory Forensics

- RAM = Random Access Memory
- Volatile memory for program code and data
- Main type in PCs: D(ynamic) RAM
  -> needs frequent refresh
- Second type: S(tatic) RAM
  -> keeps content while powered



Why RAM Forensics?

In general: RAM dump may contain data never stored to permanent memory, for example:

- Passwords / encryption keys
- Volatile user input (e.g. browser “private“ mode)
- Traces of buffer overflows and similar exploits
- RAM-only rootkits / viruses

PERSISTENCE MECHANISM

The Duqu 2.0 malware platform was designed in a way that survives almost exclusively in memory of the infected systems, without need for persistence. To achieve this, the attackers infect servers with high uptime and then re-infect any machines in the domain that get disinfected by reboots. Surviving exclusively in memory while running kernel level code through exploits is a testimony to the technical prowess of the group. In

The Pros and Cons

Pros

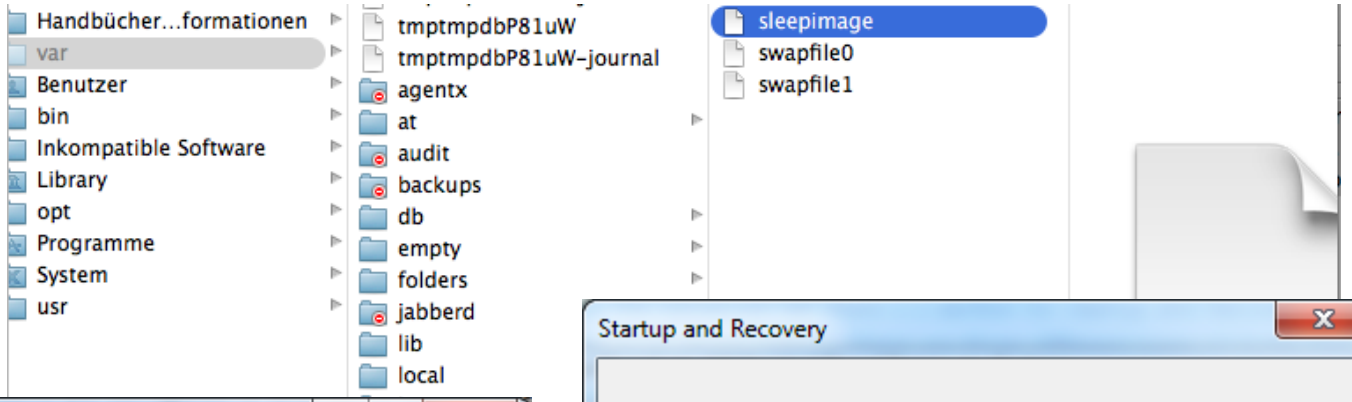
- Get access to non-persistent data
- Deep insight into system operation
- “Bypasses“ full-disk encryption etc.

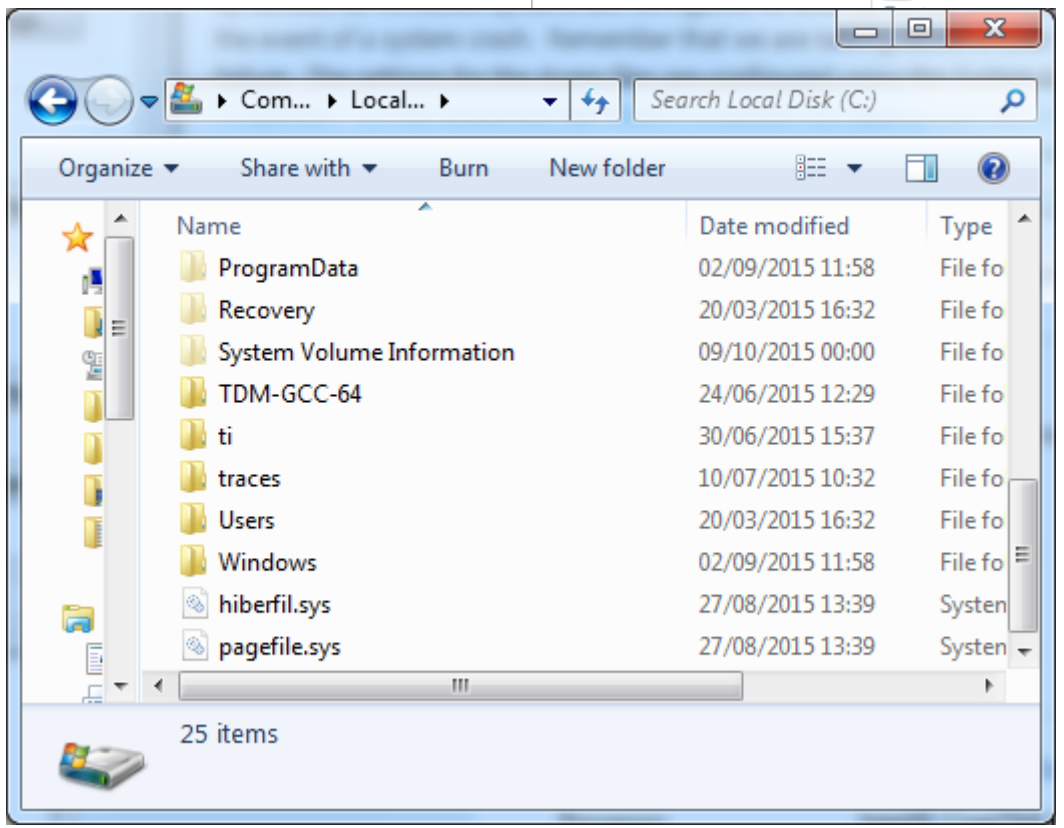
Cons

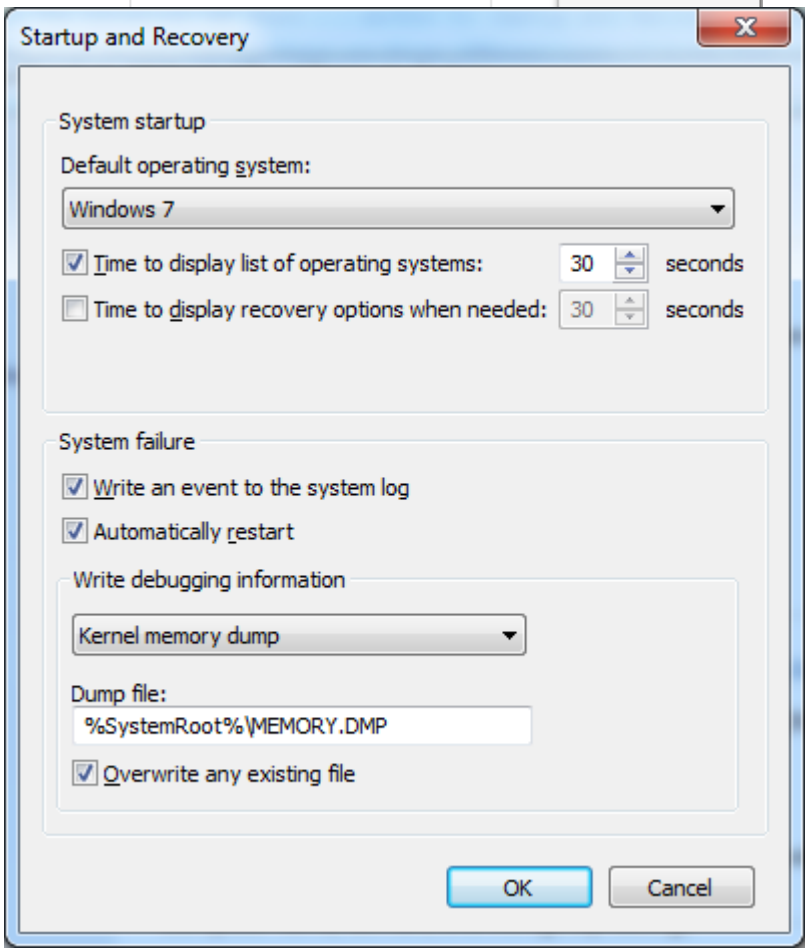
- Harder to obtain dumps (compared to HDDs etc.)
- Dump more likely to change system
- More complicated analysis (vs. HDDs)

How to dump RAM?

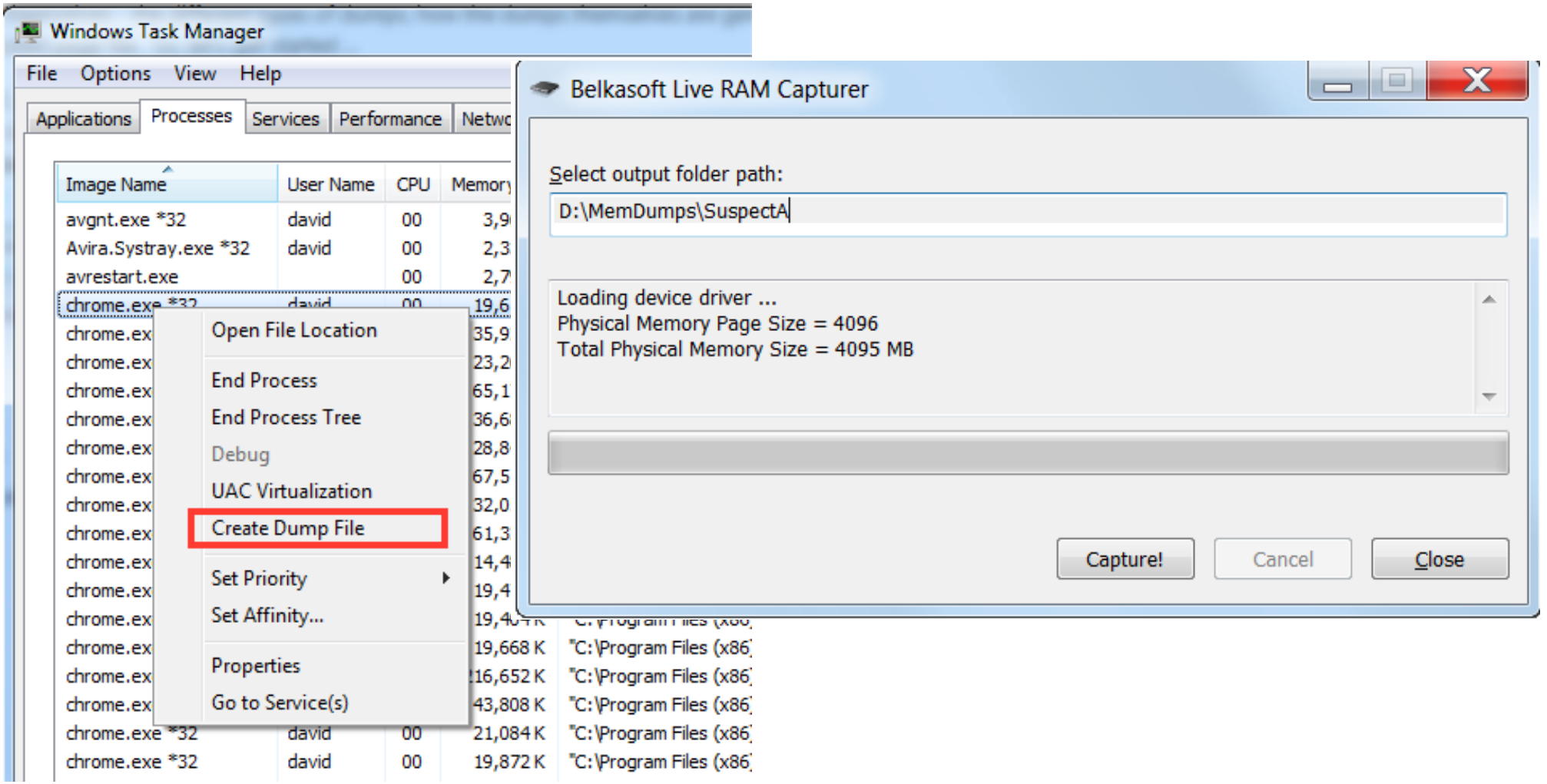
Crash Dumps / Swap & Hibernation Files







Software for Memory Dumps (Windows)



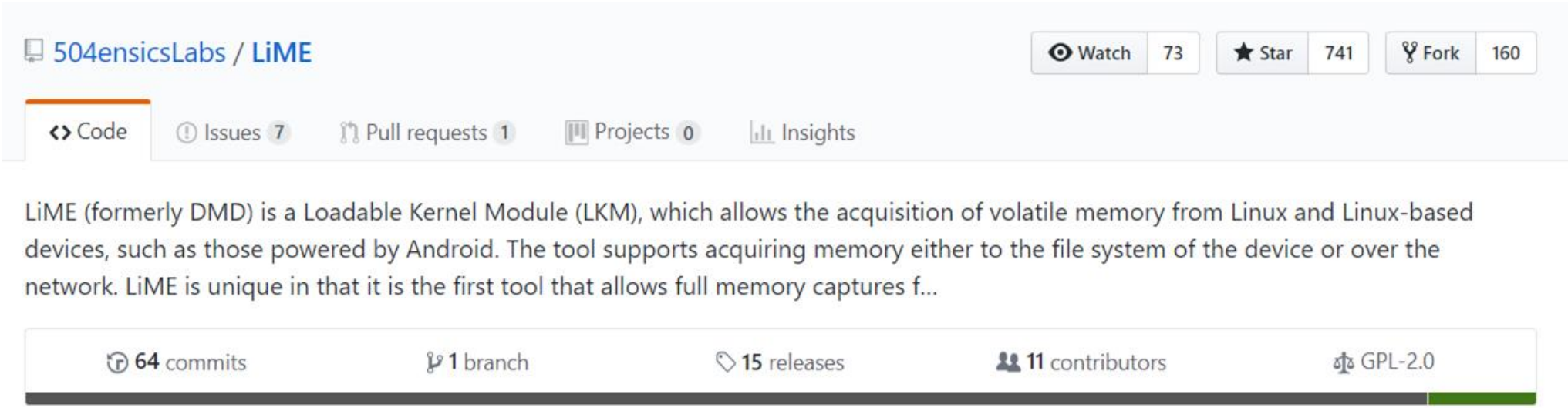
Software for Memory Dumps (Linux)

See e.g. https://stackoverflow.com/a/23001686:

`/proc/<proc_id>/maps`: List of mapped memory regions

`/proc/<proc_id>/mem`: Respective memory contents

or:



https://github.com/504ensicslabs/lime

Exploits for Memory Dumps

Again, we leaked 12 MB of kernel memory to measure the performance. With exception suppression, we achieved average reading speeds of 503 KB/s. Moreover, the error rate of 0.02 % with exception suppression is even lower than with exception handling. Thus, the channel capacity we achieve with exception suppression is 502 KB/s.

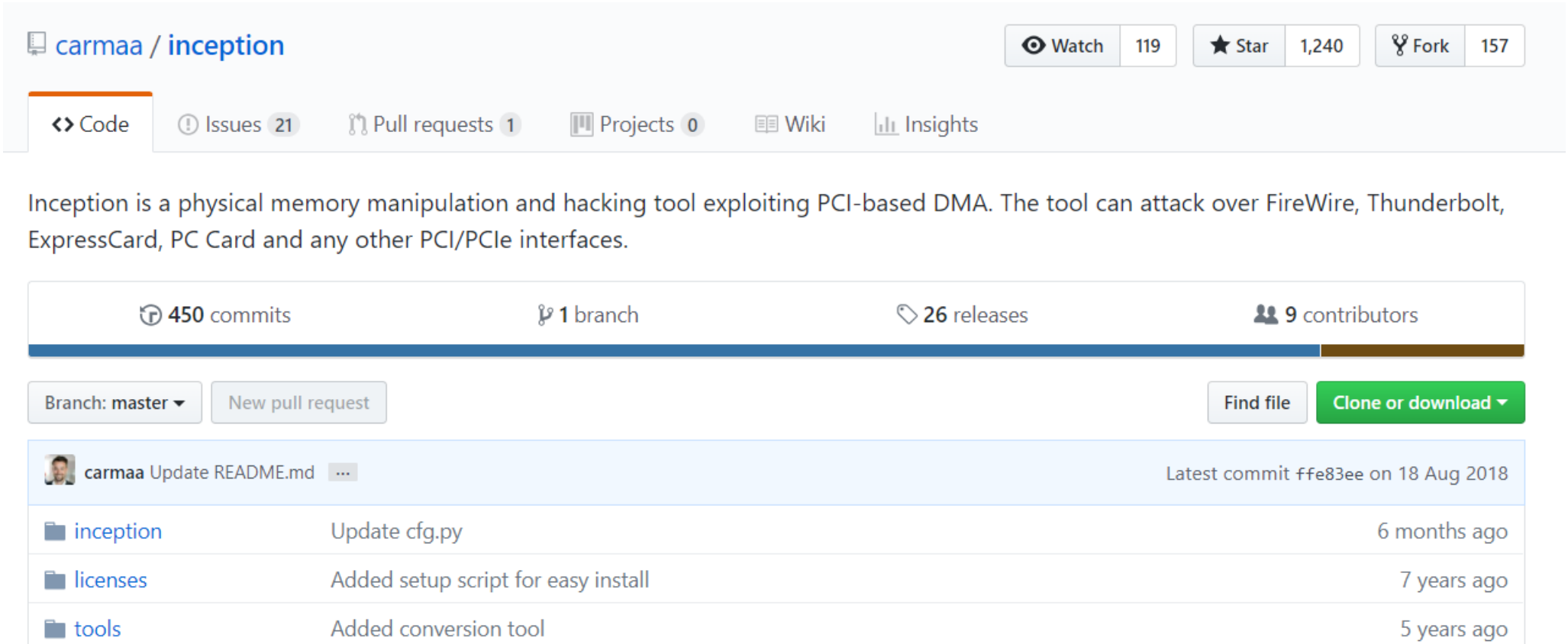
Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with

Hardware for Memory Dumps

- DMA = Direct Memory Access
- Exposed via: PCIe, Firewire, Thunderbolt, ExpressCards, ...



carmaa / inception

Watch 119 | Star 1,240 | Fork 157

Code | Issues 21 | Pull requests 1 | Projects 0 | Wiki | Insights

Inception is a physical memory manipulation and hacking tool exploiting PCI-based DMA. The tool can attack over FireWire, Thunderbolt, ExpressCard, PC Card and any other PCI/PCIe interfaces.

450 commits | 1 branch | 26 releases | 9 contributors

Branch: master | New pull request | Find file | Clone or download

carmaa Update README.md ... Latest commit ffe83ee on 18 Aug 2018

inception	Update cfg.py	6 months ago
licenses	Added setup script for easy install	7 years ago
tools	Added conversion tool	5 years ago

Hardware for Memory Dumps

- “[OS X > 10.7.2] and [Windows > 8.1] disables FireW… he OS and t…
- “[OS … = 2012 Macs… cking DMA … modu… ’.
- But: t… ercial soluti… be now …

Technical Surveillance Units and Forensic Experts often face a situation where they need to access a running computer system without shutting it down in order to prevent data loss or save essential time during an operation. In most cases, the Target System is protected with a **password-enabled Screensaver** or the target user is not logged in and the **Login Screen** is active.

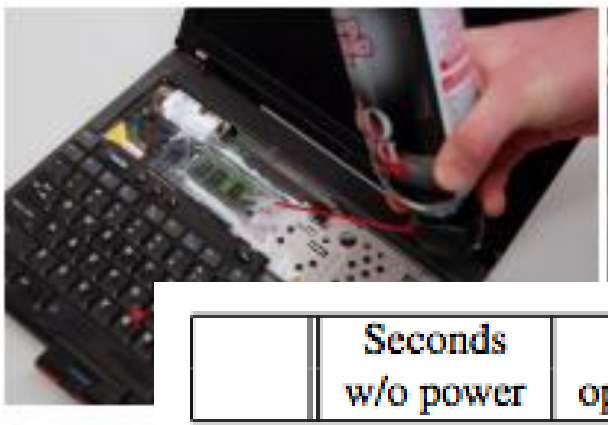
FinFireWire enables the Operator to quickly and covertly **bypass the password-protected** screen and access the Target System without leaving a trace or harming essential forensic evidence.

Cold Boot Attacks

- RAM keeps state longer after power-down if cooled (the colder the better)

  Halderman et al. “Lest We Remember: Cold Boot Attacks on Encryption Keys“, USENIX ’08
- Use freezer spray to cool to -50° C, then
- Either boot minimal dump OS …
- … or transfer DIMM modules to “dump“ machine

Cold Boot Attacks (2)



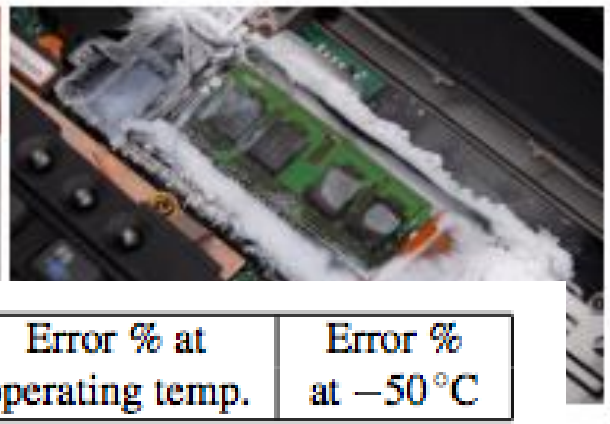


Figure 5: E
memory ch
with minin

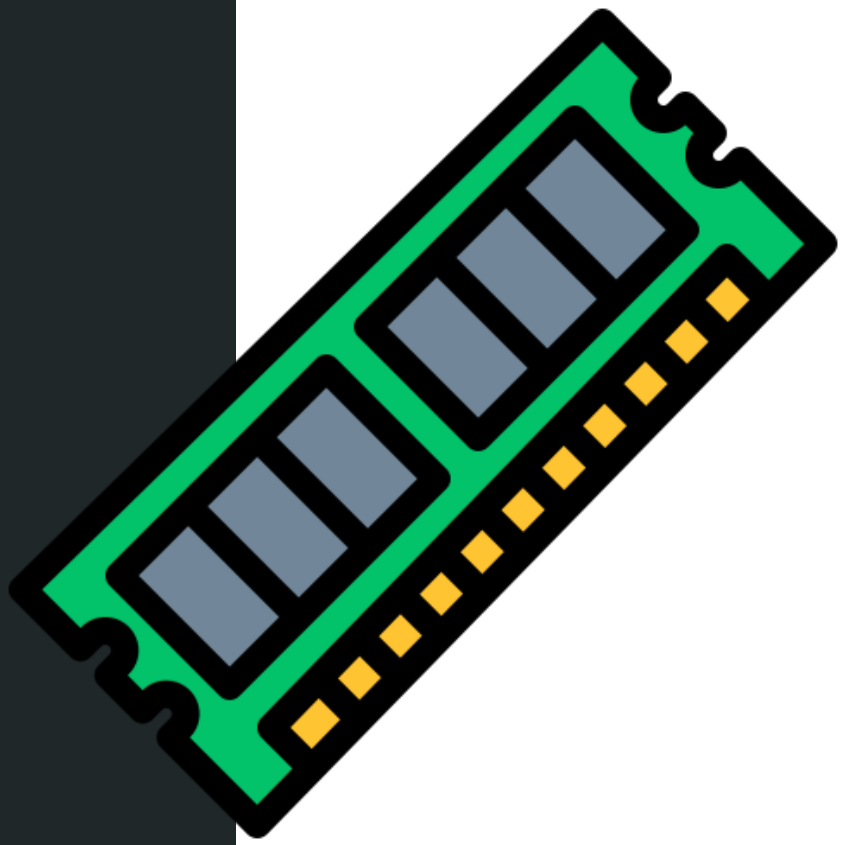
ter of multipurpose duster directly onto the
persist for several minutes after power loss

	Seconds w/o power	Error % at operating temp.	Error % at −50 °C
A	60	41	(no errors)
	300	50	0.000095
B	360	50	(no errors)
	600	50	0.000036
C	120	41	0.00105
	360	42	0.00144
D	40	50	0.025
	80	50	0.18

Table 2: Effect of cooling on error rates

Halderman et al. “Lest We Remember: Cold Boot Attacks on Encryption Keys“, USENIX ’08

Analyzing RAM dumps



Basic Approach

- `strings` utility
- Hex editor (if you know what you look for)
- Special-purpose tools to find cryptographic keys or other information:
  - Keys: aeskeyfind and others https://citp.princeton.edu/research/memory/code/
  - Images: http://w00tsec.blogspot.co.uk/2015/02/extracting-raw-pictures-from-memory.html

Problems and Caveats

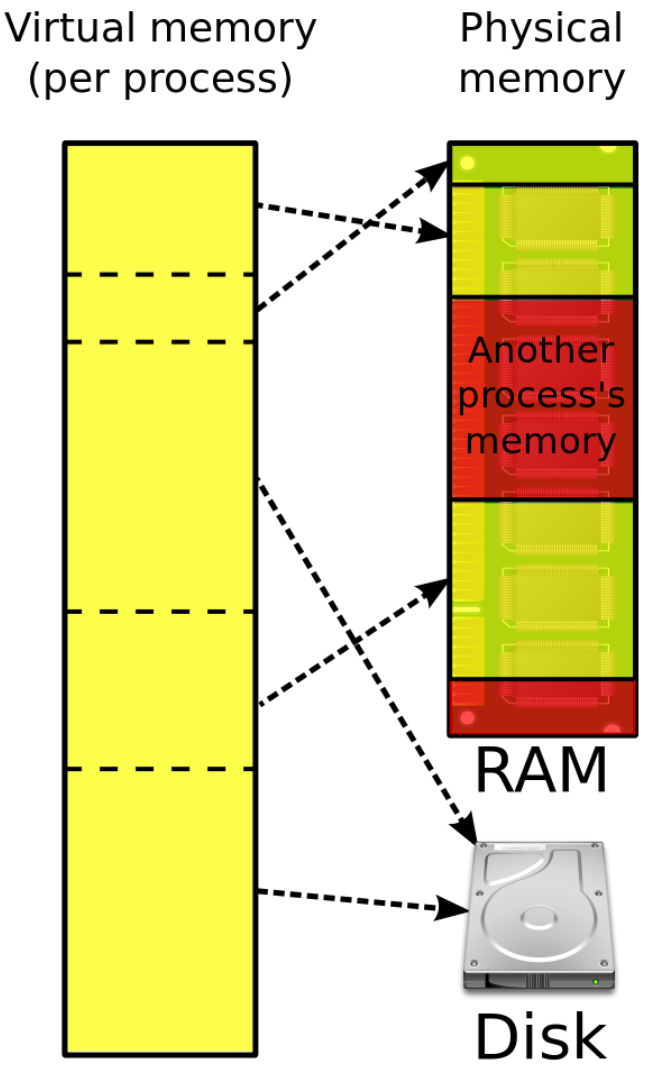
- Different types of dumps
  - Process dump (only one process)
  - Swap files (need to understand format)
  - Raw physical RAM (virtual vs. physical memory)

- How do modern OSes handle memory?
  - concept of virtual memory

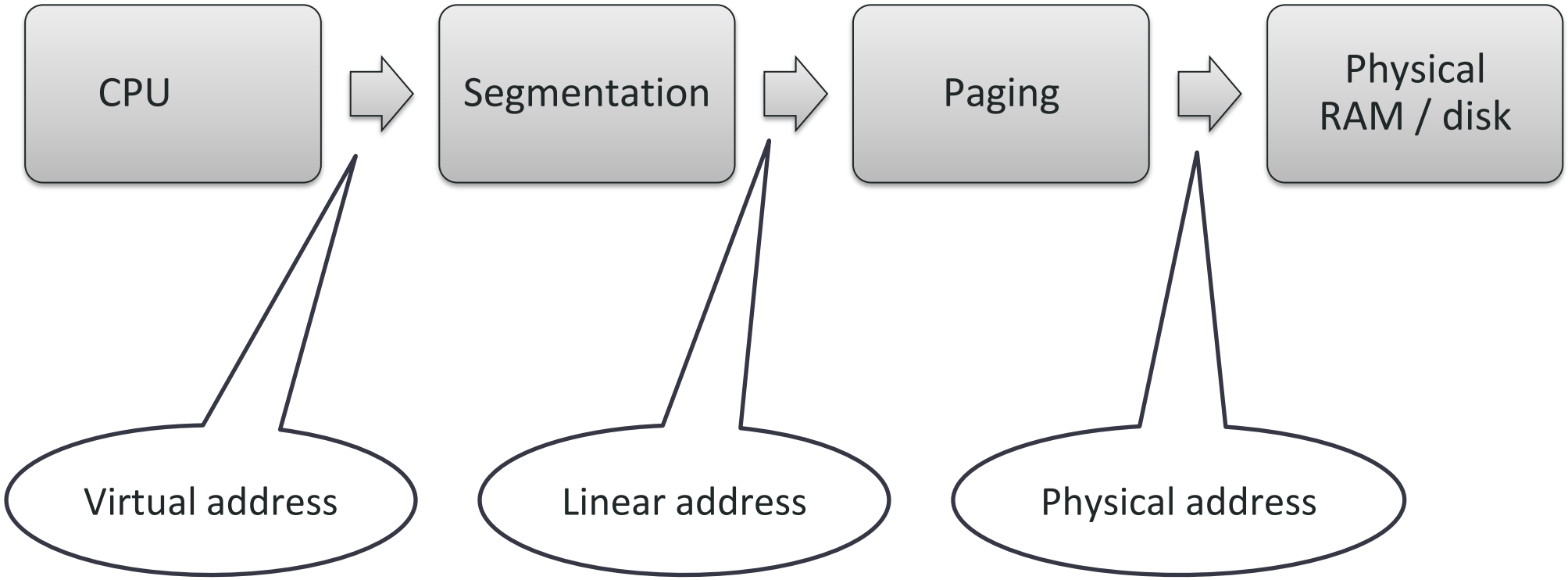
Virtual Memory 101

Let's assume 32-bit for simplicity:

- Each process has 4 GB (2^{32}) **virtual memory**
- Need to map virtual address to physical location in RAM
- Can also use disk (swapfile)
- Further reading:
  http://resources.infosecinstitute.com/translating-virtual-to-physical-address-on-windows-segmentation/



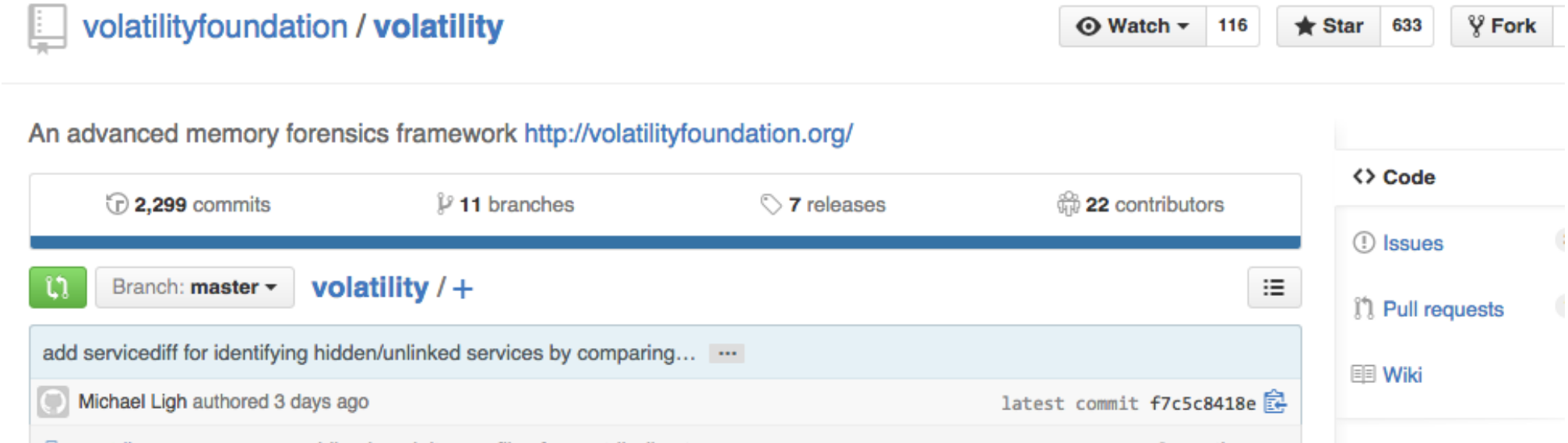
Address Translation Overview



Segmentation not used in modern OSes, i.e.
virtual addr == linear addr
Mostly removed in x86_64

Virtual Memory and Forensics

- Virtual memory hardware-supported by MMU (memory management unit)
- Need to restore virtual memory if physical dump given
- Luckily, there are tools (we'll see in the lab)



Next part: Mobile Forensics