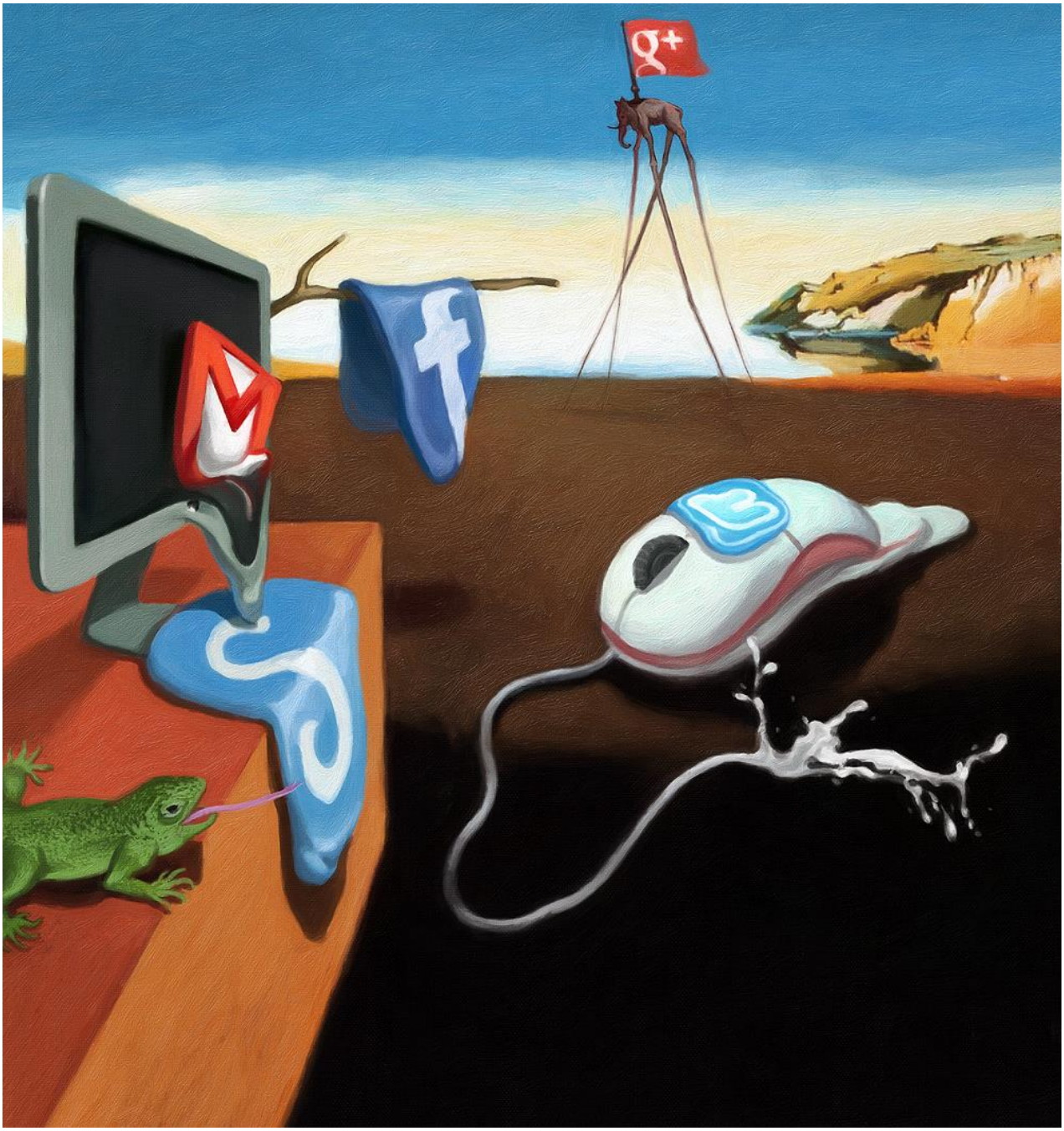
Catching the ghost: how to discover ephemeral evidence with Live RAM analysis

Oleg Afonin and Yuri Gubanov, contact@belkasoft.com



Belkador Dali. "Losing volatile Evidence".
All rights reserved.

Contents

Ephemeral Evidence

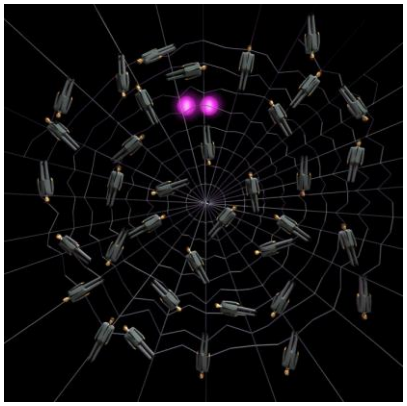
Until very recently, it was a standard practice for European law enforcement agencies to approach running computers with a "pull-the-plug" attitude without recognizing the amount of evidence lost with the content of the computer's volatile memory. While certain information never ends up on the hard drive, such as ongoing communications in social networks, data on running processes or open network connections, some other information may be stored securely on an encrypted volume. By simply pulling the plug, forensic specialists will slam the door to the very possibility of recovering these and many other types of evidence.

The Role of Live RAM Analysis in Today's Digital Forensics

Capturing and analyzing volatile data is essential for discovering important evidence. Making a RAM dump should become a standard operating procedure when acquiring digital evidence before pulling the plug and taking the hard drive out.

Types of Evidence Available in Volatile Memory

Many types of evidence are available in computer's volatile memory that can be extracted by analyzing memory dumps. Volatile and ephemeral evidence types include:



- Running processes and services;
- Unpacked/decrypted versions of protected programs;
- System information (e.g. time lapsed since last reboot);
- Information about logged in users;
- Registry information;
- Open network connections and ARP cache;
- Remnants of chats, communications in social networks and MMORPG games;
- Recent Web browsing activities including IE InPrivate mode and similar privacy-oriented modes in other Web browsers;
- Recent communications via Webmail systems;
- Information from cloud services;
- Decryption keys for encrypted volumes mounted at the time of the capture;
- Recently viewed images;
- Running malware/Trojans.

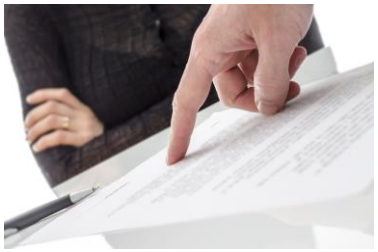
Limitations of Volatile Memory Analysis

Realistically, Live RAM analysis has its limitations, lots of them. Many types of artifacts stored in the computer's volatile memory are ephemeral: they're here once, gone the next minute. While information about running processes will not go anywhere until they are finished, remnants of recent chats, communications and other user activities may be overwritten with other content any moment the operating system demands yet another memory block.

Investigators should expect to extract remnants of recent user activities, parts and bits of chats and conversations, etc. Essentially, only recent information will still be available in the content of volatile memory.

Collecting Volatile Data that Can Withstand Legal Scrutiny

Legal, organizational and technical aspects of data acquisition are all equally important when acquiring ephemeral evidence.



The choice of tools and methods of capturing volatile data is extremely important. The choice of a wrong tool or an improper use of the right one may render the entire acquisition useless (more on that later). An attempt to use an inappropriate tool may not only fail to produce meaningful results, but to irreversibly destroy existing evidence.

It is essential to realize that acquiring volatile memory will inevitably leave acquisition footprint. While this may seem acceptable to the law enforcement officer performing the acquisition, convincing the court will be a different matter. Proper documentation of every step of the acquisition process is essential for collecting evidence that can withstand legal scrutiny.

Acquisition Footprint

In order to acquire the content of the computer's volatile memory, the investigator will have to execute a memory dumping tool, thus inevitably leaving an acquisition footprint both in the volatile memory and on the computer's hard disk. Therefore, it is essential to carefully weigh the benefits of RAM acquisition against such drawbacks, taking into account that dumping live RAM contents might be the only way to obtain certain types of evidence (including, for example, decryption keys used to access to encrypted disk volumes that may contain orders of magnitude more evidence than RAM alone).

Currently, most court systems are ready to recognize the fact that certain footprint is introduced by law enforcement during the acquisition process. For that to be the case, the entire acquisition process must be carefully documented.

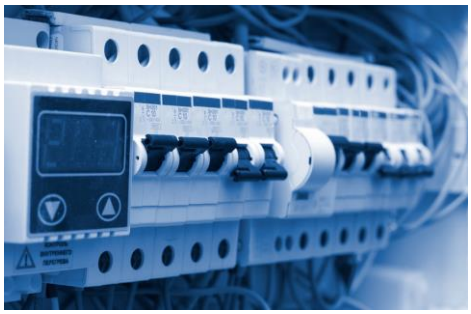
Live Box vs. Offline Analysis

Performing analysis of a running computer requires a careful assessment of risk vs. potential benefits. The first step of live box analysis should always involve capturing a memory dump for off-line analysis. Should anything go wrong during the investigation of a running computer, the memory dump can still be analyzed. After taking a memory dump, continuing with live box analysis may be beneficial if, for example, there is certain information stored on remote servers, and a network connection (e.g. a secure VPN connection or an RDP session) is established which may be lost when the computer is plugged off.

Standard Procedure

The official ACPO Guidelines recommend the following standard procedure for capturing a memory dump:

- Perform a risk assessment of the situation: Is it evidentially required and safe to perform volatile data capture?
- If so, install volatile data capture device (e.g. USB Flash Drive, USB hard drive etc.)
- Run the volatile data collection script.
- Once complete, stop the device (particularly important for USB devices which if removed before proper shutdown can lose information).
- Remove the device.
- Verify the data output on a separate forensic investigation machine (not the suspect system).
- Immediately follow with standard power-off procedure.

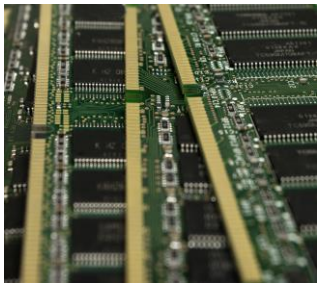


Tools and Techniques for Capturing Memory Dumps

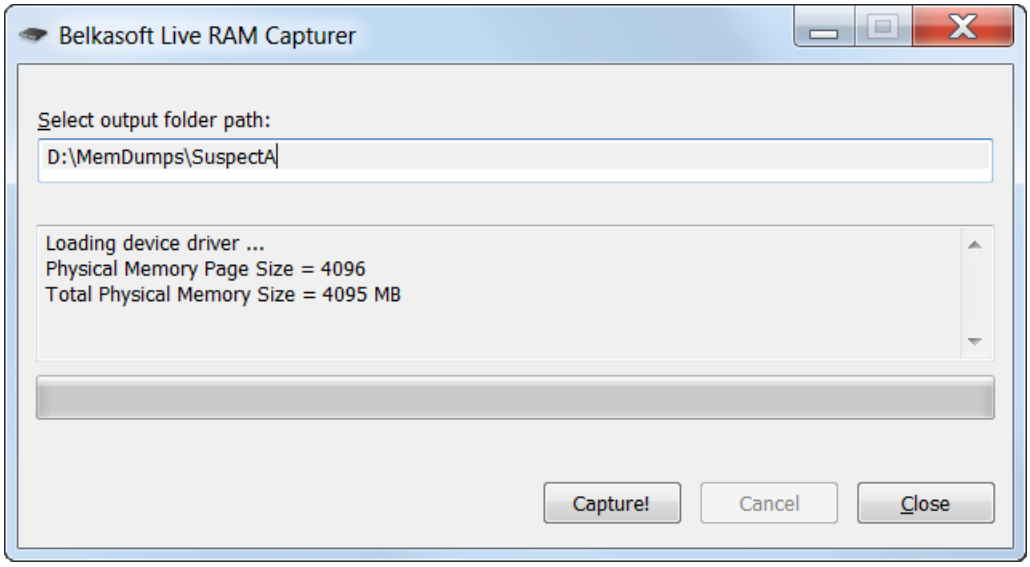
A range of tools and methods are available to capture memory dumps. From the forensic perspective, there are certain requirements that any such tool must strictly conform to. In no particular order, the list of essential requirements goes like this.

1. Kernel-mode operation;
2. Smallest footprint possible;
3. Portability;
4. Read-only access.

Kernel-mode operation is essential for a forensic memory capturing tool. With many applications proactively protecting their memory sets against dumping, running a memory acquisition tool that operates in user-mode is simple suicide. At best, such tools will read zeroes or random data instead of the actual information. In a worst-case scenario, a proactive anti-debugging protection will take immediate measures to effectively destroy protected information, then lock up and/or reboot the computer, making any further analysis impossible.



For this not to happen, investigators must use a proper memory acquisition tool running in the system's most privileged kernel mode. Notably, current versions (as of April 24, 2014) of two popular forensic memory dumping tools, AccessData FTK Imager and PMDump, run as user-mode applications and are unable to overcome protection imposed by anti-debugging systems operating in a privileged kernel mode.



The **smaller footprint** is left by a memory acquisition tool, the better. Using a tool like that already leaves traces and potentially destroys certain evidence. The less of this, the better.

Memory dumping tools must be **portable**, ready to run from an investigator-provided device (e.g. USB flash drive or a network location). Tools requiring installation are inadmissible for obvious reasons.

Finally, any sane forensic tool would never write anything onto the disk of the computer being analyzed, will not create or modify Registry values, etc.

Belkasoft makes a tool that complies with all the requirements: **Belkasoft RAM Capturer**. The tool comes with 32-bit and 64-bit Windows drivers, allowing it to dump proactively protected memory content in kernel mode.

Consequences of Choosing the Wrong Tool

Many types of computer games, chat rooms, encryption programs and malware are known to be using some sort of anti-dumping protection. In mild scenarios (e.g. commercial products and games), an attempt to read a protected memory area will simply return empty or garbage data instead of the actual information.

In worst-case scenarios, an anti-debugging system detecting an attempt to read protected memory areas may take measures to destroy affected information and/or cause a kernel mode failure, locking up the computer and making further analysis impossible. This is what typically happens if a user-mode volatile memory analysis tool is used to dump content protected with a kernel-mode anti-debugging system.

The FireWire Attack

One technique in particular allows capturing the computer's RAM without running anything foreign on the system. This technique works even if a computer is locked, or if no user is logged on. The FireWire attack method [1] is based on a known security issue that impacts FireWire / i.LINK / IEEE 1394 links. One can directly acquire the computer's operating memory (RAM) by connecting through a FireWire link.

What makes it possible is a feature of the original FireWide/IEEE 1394 specification allowing unrestricted access to PC's physical memory for external FireWire devices via Direct Memory Access (DMA). As this is DMA, the exploit is going to work regardless of whether the target PC is locked or even logged on. There's no way to protect a PC against this except explicitly disabling FireWire drivers. The vulnerability exists for as long as the system is running. Multiple tools are available to carry on this attack.

Note that the use of this technique has certain requirements. The technique either requires that the computer has a FireWire port and working FireWire drivers are installed (and not disabled) in the system, or makes use of a hot-pluggable device adding FireWire connectivity to computers without one. For example, a PCMCIA/Cardbus/ExpressCard slot in a laptop can be used to insert one of the popular Firewire add-on cards. There is a high probability that the operating system will automatically load the driver for that card, allowing the attacker to use the card for performing a FireWire attack. [3]

Sources such as [3] even describe techniques allowing using an iPhone as a FireWire capturing device!

The "Freezer Attack" on Scrambled Smartphones

An ordinary household freezer has been successfully used to attack encrypted smartphone's memory content after the phone has been turned off [2].

After the release of Android 4.0, smartphones running the new OS gained the ability to encrypt (scramble) data stored on user partitions. This security feature protects user's information against attacks bypassing screen locks.

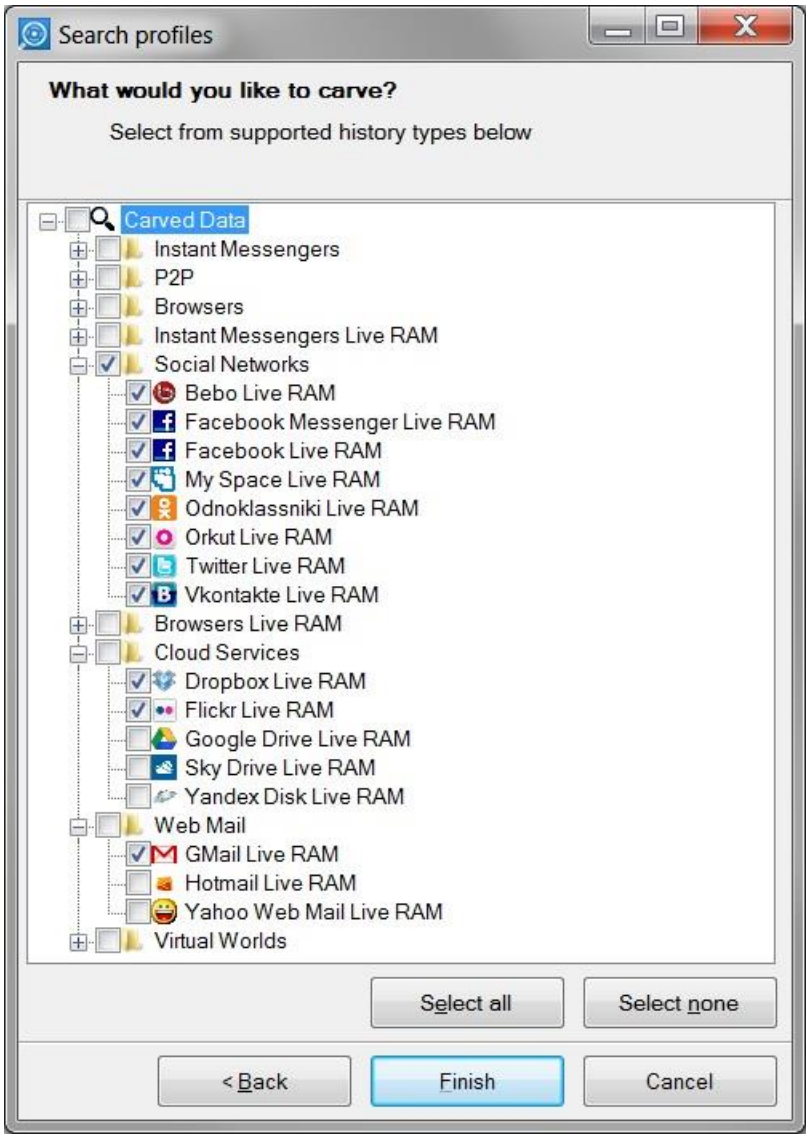
Disk decryption keys are stored in the phone's volatile memory, and can be retrieved by performing a cold boot, as demonstrated by German researchers. The idea is cooling the smartphone down to a low temperature (about -15 degrees Celsius) in order to slow down the process of RAM contents fading away. Cooled down phones are then reset into "fastboot" mode, then connecting the phone to a PC with custom-developed FROST "fastboot" software installed. The software allows searching for volume decryption keys, perform a RAM memory dump, and crack screen lock keys (4-digit PINs only).

FROST software and step-by-step instructions can be downloaded from https://www1.informatik.uni-erlangen.de/frost

Tools for Analyzing Memory Dumps

At this time, no single forensic tool can extract *all* possible artifacts from a memory dump. Different tools are used to analyze chat remnants, lists of running processes or extract decryption keys for encrypted volumes mounted at the time of the capture. A brief list of such analysis tools is available below.

Belkasoft Evidence Center [http://Belkasoft.com/] : remnants of conversations and communications occurring in social networks, chat rooms, multi-player online games, Skype; data from cloud services such as Flickr, Dropbox, Sky Drive, Google Drive etc.; communications in Webmail systems such as Gmail, Hotmail, Yahoo; Web browser and virtual worlds artifacts, and so on.



Elcomsoft Forensic Disk Decryptor [http://elcomsoft.com/]: extracts decryption keys protecting encrypted volumes (PGP, True Crypt, BitLocker and Bitlocker To Go containers are supported), allowing investigators to instantly access the content of these encrypted volumes without brute-forcing the original volume password. All the keys from a memory dump are extracted at once, so if there is more than one crypto container in the system, there is no need to re-process the memory dump.

Passware [http://passware.com]: forensic toolkit including tools for capturing memory dumps via FireWire attack. Also includes a tool to extract decryption keys for popular crypto containers.

About the Authors

Yuri Gubanovis a renowned computer forensics expert. He is a frequent speaker at industry-known conferences such as EuroForensics, CEIC, China Forensic Conference, FT-Day, ICDDF, TechnoForensics and others. Yuri is the Founder and CEO of Belkasoft. Besides, Yuri is an author of f-interviews.com, a blog where he takes interviews with key persons in digital forensics and security domain.You can add Yuri Gubanov to your LinkedIn network at http://linkedin.com/in/yurigubanov

Oleg Afonin is Belkasoft sales and marketing director. He is an expert and consultant in computer forensics.

Contacting the Authors

You can contact the authors via email: contact@belkasoft.com

About Belkasoft Research

Belkasoft Research is based in St. Petersburg State University. The company performs non-commercial researches and scientific activities.

About Belkasoft

Belkasoft
forensics made easier

Founded in 2002, Belkasoft is an independent software vendor specializing in computer forensics and IT security software. Belkasoft products back the company's "Forensics made easier" slogan, offering IT security experts and forensic investigators solutions that work right out of the box, without requiring a steep learning curve or any specific skills to operate.

Belkasoft Evidence Center 2013 is a world renowned tool used by thousands of customers for conducting forensic investigations, as well as for law enforcement, intelligence and corporate security applications. Belkasoft customers include government and private organizations in more than 40 countries, including the FBI, US Army, DHS, police departments in Germany, Norway, Australia and New Zealand, PricewaterhouseCoopers, and Ernst & Young.

References

[1] The FireWire attack method existed for many years, but for some reason it's not widely known. This method is described in detail in many sources such as http://www.securityresearch.at/publications/windows7_firewire_physical_attacks.pdf or http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation

[2] FROST: Forensic Recovery Of Scrambled Telephones https://www1.informatik.uni-erlangen.de/frost

[3] Physical memory attacks via Firewire/DMA - Part 1: Overview and Mitigation (Update) | Uwe Hermann http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation