VILNIUS TECH
Vilniaus Gedimino technikos universitetas

Cyber Forensics

Lab work No. 2

2025-2026 fall semester

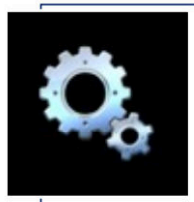
Tools, tools, tools

RAM Collection

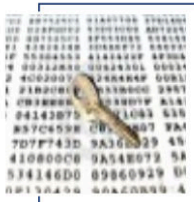
Processes

Network connections

Open files, Registry keys, and devices

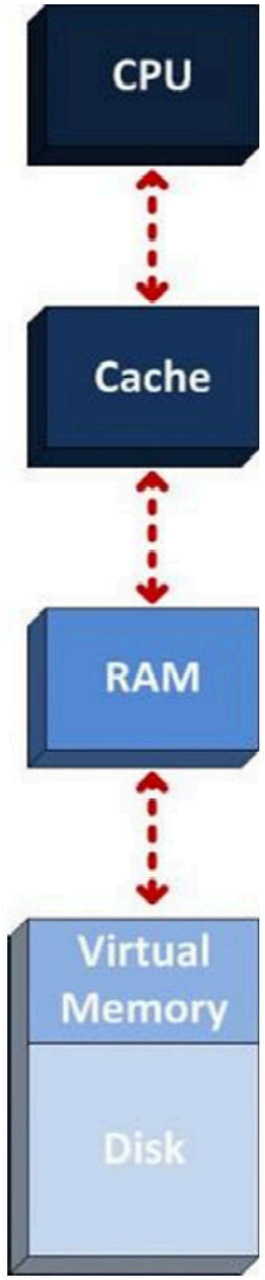


Configuration parameters



Encryption keys and passwords

Memory-only exploits/rootkit technology



Everything in the OS traverses RAM:

- Processes and threads
- Malware (including rootkit technologies)
- Network sockets, URLs, IP addresses
- Open files
- User-generated content
  - Passwords, caches, clipboards
- Encryption keys
- Hardware and software configuration
- Windows registry keys and event logs

Memory Analysis Advantages

- Best place to identify malicious software activity
  - Study running system configuration
  - Identify inconsistencies (contradictions) in system
  - Bypass packers, binary obfuscators, rootkits (including kernel mode), and other hiding tools
- Analyze and track recent activity on the system
  - Identify all recent activity in context
  - Profile user or attacker activities
- Collect evidence that cannot be found anywhere else
  - Memory-only malware
  - Chat threads
  - Internet activities

Memory forensics

- In-memory detections provide advanced capabilities:
  - Process Information
  - Command line artifacts
  - Network activity
  - Process handles and execution tracing
  - Windows API Usage
  - DLL injection and hooking (rootkit) detection
  - Thread creation and memory allocation
- Easy detection of many PS, WMI and fileless attacks

Memory Acquisition Tools

- Surge - Volexity's Surge Collect offers flexible storage options and an intuitive interface that any responder can run to eliminate the issues associated with the corrupt data samples, crashed target computers, and ultimately, unusable data that commonly results from using other tools.
- MAGNET RAM - MAGNET RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer, allowing investigators to recover and analyze valuable artifacts that are often only found in memory.
- FTK Imager - FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Forensic Toolkit (FTK®) is warranted.
- Winpmem - WinPmem has been the default open source memory acquisition driver for windows for a long time.
- Ram Capturer - Belkasoft Live RAM Capturer is a tiny free forensic tool that allows to reliably extract the entire contents of computer's volatile memory—even if protected by an active anti-debugging or anti-dumping system.
- LiME - A Loadable Kernel Module (LKM) which allows for volatile memory acquisition from Linux and Linux-based devices, such as Android.
- AVML - AVML is an X86_64 userland volatile memory acquisition tool written in Rust, intended to be deployed as a static binary.
- fmem - This module creates /dev/fmem device, that can be used for dumping physical memory, without limits of /dev/mem (1MB/1GB, depending on distribution).
- FEX Memory Imager - FEX Memory Imager (FEX Memory) is a free imaging tool designed to capture the physical Random Access Memory (RAM) of a suspect's running computer. This allows investigators to recover and analyze valuable artifacts found only in memory.
- MacQuisition
- Digital Collector - A powerful forensic imaging software solution to perform triage, live data acquisition and targeted data collection for Windows and Mac computers.

Memory Analysis Tools

- Volcano - A comprehensive, cross-platform, next- generation memory analysis solution, Volexity Volcano Professional's powerful core extracts, indexes, and correlates artifacts to provide unprecedented visibility into systems' runtime state and trustworthiness.
- Volatility3 - Volatility is the world's most widely used framework for extracting digital artifacts from volatile memory (RAM) samples.
- MemProcFS - The Memory Process File System (MemProcFS) is an easy and convenient way of viewing physical memory as files in a virtual file system.
- WinDbg - The Windows Debugger (WinDbg) can be used to debug kernel-mode and user-mode code, analyze crash dumps, and examine the CPU registers while the code executes.
- Volatility - The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples.
- Volafox - macOS Memory Analysis Toolkit' is developed on Python 2.x (Deprecated)
- Rekall - A new branch within the Volatility project was created to explore how to make the code base more modular, improve performance, and increase usability. (Deprecated)
- Redline - Redline®, FireEye's premier free endpoint security tool, provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and the development of a threat assessment profile.
- Memoryze - Mandiant's Memoryze™ is free memory forensic software that helps incident responders find evil in live memory. Memoryze can acquire and/or analyze memory images and on live systems can include the paging file in its analysis.
- dwarf2json - Go utility that processes files containing symbol and type information to generate Volatilty3 Intermediate Symbol File (ISF) JSON output suitable for Linux and macOS analysis.

General goals

- If you receive for examination the device involved in the incident, there is a high probability that it is either one of the following:
  - The alleged victim's device
  - The suspect's device

The victim's device

- Consider a situation in which the victim's device is under investigation. The main goal in this case is to answer the question, What happened? One way is to break this question down into its components:
  - 1. How did an attacker gain access to the system?
  - 2. What tools were launched?
  - 3. Did the attacker get persistence?
  - 4. Was there a lateral movement?
  - 5. What actions on the objective were performed?

- Now do the same thing with the question, *How did the attacker gain access to the system?*:
  - 1. Are there any traces of potentially malicious files/links having been opened?
  - 2. Are there any remote connection services running?
  - 3. Are there any traces of suspicious connections?
  - 4. Are there any traces of removable devices being connected?

- Let's ask questions about malicious files too:
  - 1. Are there any traces of suspicious files saved?
  - 2. Are there any traces of suspicious links opened?
  - 3. Are there any traces of suspicious files opened?

The suspect's device

- A similar method can be used to investigate the device from which the attacks are suspected to have originated. In this case, questions would be posed based on what the owner of the device is suspected of. For example, if owner is suspected of being a malware developer, questions would be related to the presence of development tools, traces of source code, sales of malware, and so on.

Two options for this assignment

1. Volatile and Non-volatile memory forensic analysis.
2. Belka CTF ReRun on Magnet Axiom.

First option

Memory analysis

Volatile and Non-volatile memory forensic analysis.

Tools for practical work*

- The Volatility Framework (with plugins for Linux);
- FTK Imager;
- Arsenal Image Mounter;
- Autopsy;
- Kali;
- Velociraptor;
- Backtrack;
- Magnet Axiom;
- Belkasoft;
- DFF;
- Mdd;
- Win86/64dd;
- DumpIt;
- WinPmem.

Any other toolset for memory acquirement and analysis.

* Tools for work can be chosen freely according to your requirements.

* This list should be considered only as example.

Practical work will include:

- Memory Forensic challenge.
- Analysis of remnants, malware, breach artefacts.

Complex Memory Forensic challenge: Briefing

- As a forensic examiner you will get (**TEAMS>Files**):
  - Server Disk Image.
  - Server Memory Image.
- What is known:
  - Server was compromised.
- What is unknown:
  - What actually happened.

Memory Forensic Challenge Questions

- From what kind of system dumps were taken from?
- What processes were running?
- Whether the system issued any alerts/warnings?
- When the server has been breached?
- What was the attack vector?
- What user/account was used for a breach?
- What service was used for the attack?
- What specific attacks were used against machine?
- What network connections were open during attack?
- How successful were the attacks?
- Can you recover any files related to the breach?
- Can you recreate full timeline of the incident?
- What was taken?
- What is the server IP?
- What IP did hacker use?
- What tools (you think/know) were used for the attack?
- What action could have saved the server from attack?
- What can you say about attacker’s expertise level, skills?
- Can you create PoC to simulate incident? If so, replicate it.

What you need to prepare for the assessment (first option):

- **Mandatory part :**
  - Complete the work, be ready to take a test.
  - **Maximum** score (mark) that you can earn by this part is – **7 points.**

- **A continuous (optional part):**
  - Prepare a short demonstration of work results (recovery process, recovered data, hash comparison, data analysis, information about criminals).
  - Prepare a comprehensive but concise report. Report must be submitted before the assessment. Reports are accepted only in electronic form (**PDF**).
  - **Maximum** score (mark) that you can earn with both parts is – **10 points.**

Literature for Memory Forensics

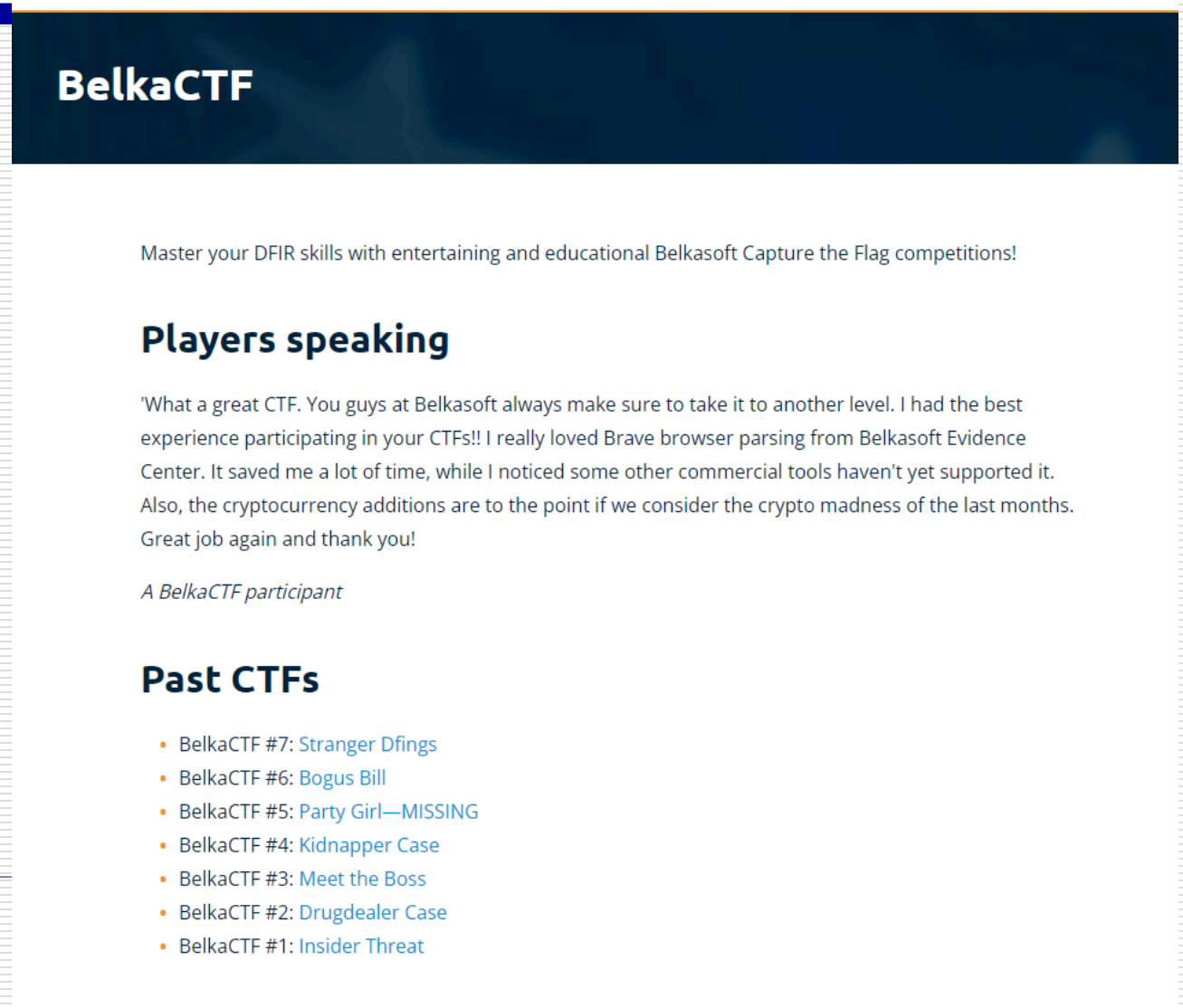
- Michael Hale Ligh, Andrew Case. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. 2014. Wiley. 912 p.
- Svetlana Ostrovskaya, Oleg Skulkin. Practical Memory Forensics: Jumpstart effective forensic analysis of volatile memory. 2022. Packt Publishing. 304 p.
- Monnappa K A . Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. 2018. Packt Publishing. 510 p.
- Dmitry Vostokov. Advanced Windows Memory Dump Analysis with Data Structures: Training Course Transcript and WinDbg Practice Exercises with Notes, Fourth Edition (Windows Internals Supplements) 4th ed. Edition. 2022. Opentask. 294 p.
- Shiva V. N. Parasram. Digital Forensics with Kali Linux: Perform data acquisition, data recovery, network forensics, and malware analysis with Kali Linux. 2020. Packt Publishing. 334 p.
- Philip Polstra. Linux Forensics. 2015. CreateSpace Independent Publishing. 370 p.

Second option

Belka CTF ReRun

https://belkasoft.com/ctf

2025-10-18



BelkaCTF

Master your DFIR skills with entertaining and educational Belkasoft Capture the Flag competitions!

Players speaking

'What a great CTF. You guys at Belkasoft always make sure to take it to another level. I had the best experience participating in your CTFs!! I really loved Brave browser parsing from Belkasoft Evidence Center. It saved me a lot of time, while I noticed some other commercial tools haven't yet supported it. Also, the cryptocurrency additions are to the point if we consider the crypto madness of the last months. Great job again and thank you!

A BelkaCTF participant

Past CTFs

- BelkaCTF #7: Stranger Dfings
- BelkaCTF #6: Bogus Bill
- BelkaCTF #5: Party Girl—MISSING
- BelkaCTF #4: Kidnapper Case
- BelkaCTF #3: Meet the Boss
- BelkaCTF #2: Drugdealer Case
- BelkaCTF #1: Insider Threat

What is ReRun

- This means that you will discover and solve all Belka CTF questions, mysteries and challenges using the Magnet Axiom forensic tool.

rerun 1 of 2 **verb**

re·run (ˌ)rē-ˈrən

reran (ˌ)rē-ˈran ; **rerun; rerunning**

Synonyms of *rerun* ›

transitive verb

: to run again or anew

rerun 2 of 2 **noun**

re·run ˈrē-ˌrən (ˌ)rē-ˈrən

: the act or action or an instance of rerunning : **REPETITION**

especially : a movie or television show that is rerun

Tools for this practical work

- **Magnet Axiom;**
- ~~Belkasoft Evidence Center;~~

Important **notes** regarding this option

- One ReRun – One Belka CTF from the list.
- You can choose **no more than two** Belka CTF ReRuns **during the whole semester**.
- Only fully completed ReRuns are accepted.

What you need to prepare for the assessment (second option):

- **The main and only part :**
  - Complete the work and prepare a short demonstration of work results (Comprehensive Report or Report + live presentation).
  - **Be ready to take only theoretical-practical test** from option No.1.
  - **Maximum** score (mark) that you can earn by selecting second option for the second assignment is – **6 points.**

Additional assignment (**Not mandatory**)

- Prepare a machine (preferably VM) with investigation tools. Infect machine with malware and analyze what methods (how) malware used to infect machine with incident response and forensic tools.
- The more interesting the sample, the more interesting the results and the more fun the investigation.
- Remember to take RAM dump.
- Prepare a concise report or Live presentation.

*Eligible for part of the extra point.

- https://github.com/digitalisx/awesome-memory-forensics
- https://github.com/cugu/awesome-forensics
- https://github.com/ivbeg/awesome-forensicstools

Discussion and questions

?