FOR532: **Enterprise Memory Forensics In-Depth**

4 Day Program	24 CPEs	Laptop Required

You Will Be Able To

- Integrate Memory forensics into their investigation workflow
- Acquire Memory on single machines with Linux, Windows and MacOS
- Acquire interesting Memory parts from many machines
- Understand how Memory works
- Identify the key Memory structures
- Effortlessly walk through the memory using volshell to identify even more traces of an attack and better understand how malware can hide
- Find malware using a standardized process
- Uncover malware capabilities and configurations
- Understand which attacker actions lead to which traces in Memory
- Understand DKOM (direct kernel object manipulation)
- Understand advanced detection countermeasures that attackers apply to beat EDRs and other detection mechanisms
- Extract memory artifacts needed for the investigation
- Extract and understand user artifacts that tell you what happened on a system
- Counter ransomware actors by identifying exfiltration credentials
- Analyze Memory dumps of single processes with windbg
- Use volatility 2 and 3 to find analyze Memory images
- Understand what options malware authors have to hide the presence of malware or make investigations harder
- Analyze Memory in structured and unstructured ways
- Analyze Memory in a team approach (using centralized analysis servers)
- Write your own tools to fill the gaps of current tools
- Write your own volatility plugin
- Scale Memory forensics to thousands of machines
- Automate parts of Memory forensics
- Leverage frequency of occurence analysis (stacking) to single out machines that need a closer look

ATTACKER TRACES ARE MOST VULNERABLE IN MEMORY. TIME TO GO HUNTING!

Memory forensics is an integral part of successful incident response investigations. Over the last year, incident response procedures have grown from investigating single computer images at time to investigating hundreds of thousand machines all at once. In the beginning of every investigation, the attacker is way ahead. Incident responders need to find ways to get ahead of the attackers quickly and kick them out of our networks. While there has been a lot of light shed on scaling hard drive artifact-based investigations to large numbers of endpoints, the memory forensics part has been the neglected part of classical forensics for a while. This rapidly changes as many attacks are way more lilkely to be uncovered when looking into memory than with more classical means. Memory forensics ties into many disciplines in cyber investigations. From the classical law enforcement investigations that focus on user artifacts via malware analysis to large-scale hunting, memory forensics has several applications that for many teams are still terra incognita. The FOR532 Enterprise Memory Forensics In-Depth class strives to change that and speed up your incident response, your threat hunting, and your malware analysis significantly.

A major step to get started with memory forensics is to understand, that memory can be complex at times, but in a nutshell analyzing memory just means knowing what bytes at specific locations mean. In other terms, the better you can read the street map of memory, the more you can get out of it. For that reason, we will spend some time understanding how memory works. You will become familiar with key memory structures and what they mean.A clear understanding will help you understand how the different presented tools work and what their advantages and limitations are.

In memory forensics, the saying 'A fool with a tool is still a fool' is even more important than in classical forensics. Memory being a very dynamic kind of dataset can be easily misinterpreted which in real investigations can lead to false-negatives or send you down a rabbit hole quickly. For that reason, it is important to understand how the various tools work. Not every aspect you might need for an investigation will already be covered by a tool. Another aspect of the class is to understand what you need and how to use easy measures to get your hands on the data.

Finally, when you understand memory on one machine, it is time to scale your investigation to a larger number of machines. Both structured analysis as well as with unstructured analysis matter. We will use cutting edge toools to scale memory forensics in a unique way.

The digital evidence we leverage in the labs is designed to resemble real cases the author came across in his career. You will be working on the evidence a significant amount of time in many different labs. As it is important to understand how attackers leave certain traces, every now and then you will be asked to switch sides and attack a system that you later analyze. This approach enables incident responders to have a 360 degree view on modern incident response analysis.

In the second half of day 4 you can put your newly acquired knowledge into action in a scoreboard-style capture the flag. You will be presented with new evidence that was built based on real-world cases and score points for correctly answered questions. Regardless of how new you are to memory forensics, there will be interesting traces for you to find in the evidence.

The main goal of the class is to demonstrate, that memory forensics is not as complicated as it seems at first. You will get a set of techniques and tools to add a lot of value to your investigations by saving time and resources as well as rendering results you would not have gotten by using classical IR tactics. Add memory forensics to your toolchest now to battle evil faster and more efficiently even at scale.

Section Descriptions

SECTION 1: Fundamentals of Memory Forensics

The first step towards successful memory forensics is understanding how memory works. Even with the variety of different operating systems, how memory exists is more similar than many would think. On day 1 we will start looking into the inner workings of memory. We then move on to explore different ways of extracting memory from various operating systems (Windows and Linux, 64 and 32 bit). This includes virtual machines and techniques supporting cloud workloads. To work with memory, we will leverage volatility 2 and volatility 3 in the labs. There are differences in these versions that will clarify when it's best to use one vs. the other. We then deep-dive into memory objects using volshell to display that dereferencing memory objects is not as complicated as it might seem. Once you understand the major memory objects and their use in forensics investigations, we will investigate memory management and how that affects our investigations. Finally, we work on a five-step process to rapidly identify malware in memory. We differentiate between malware that runs as its own process and malware code that runs in the realm of another process.

TOPICS: Fundamentals of Memory, Introduction to Volatility, Understanding Memory Structures, Memory Management, Finding Malware

SECTION 3: Intrusion Forensics

Many responders think that Memory forensics is something for single host investigations. They could not be more wrong.

This part of the course focuses on scaling memory forensics. Current tools allow incident responders to scale core memory forensics techniques to thousands of machines all at once. This drastically reduces survivability of an attacker. We will introduce the memory capabilities of a tool called velociraptor which is the incident response swiss army knife that we also use in the FOR508 and FOR608 classes to demonstrate large-scale repones. Modern incident response comes with a lot of challenges. One of them is resource management. We will also shed light on when memory forensics is the right approach in an investigation and how it can be built into an IR process efficiently.

For thisreason we also dive into memory forensics automation. If you do something the same way more than twice, you should think about automating it to save time in the future. Another important point for large scale response is collaboration and knowledge transfer. We will focus on how to establish that in memory forensics.

As enterprise networks are rarely ever Windows-only, we will discuss Linux memory forensics. That is particularly important as often attackers enter the network via external facing machines and appliances. Memory might give you a quick shot to identify what is actually going on.

Sometimes it is better and faster to leverage unstructured memory analysis rather than a structured analysis. We will focus on the major techniques to apply unstructured analysis techniques locally and in scale.

TOPICS: Linux Memory Forensics; Scaling Memory Forensics; Automated Processing; Collaborative Investigations; Unstructered Memory Analys Is

SECTION 2: Diving Deeper and User Artifacts

During an intrusion, using memory analysis sometimes feels like cheating. Finding active malware should not be this easy. Malware authors spend a lot of time to hide their malware better. They have one major disadvantage. Malware can hide, but it must run. That means, that the malicious code must eventually hit the CPU in plain sight. Even well-written malware is most vulnerable in memory. On day two we start focusing on well-hidden malware that runs in the memory space of legitimate processes or even interacts directly with the kernel. You will get the chance to manually mimic malware by altering the process list using Direct Kernel Object Manipulation (DKOM). This allows you to better understand how simple hiding techniques can be and that the inner workings of an operating system are nothing monolithic where you cannot change things. We will also look at windbg which is a free Microsoft tool that supports live memory analysis and even alteration in a running operating system. You can even use it remotely over the network. A large part of the day focuses on memory-based artifacts that allow you to tell the story of an attack. Often attackers do not install malware on every endpoint they access. Instead, they jump there using legitimate tools like Remote Desktop or psexec. We, as defenders, must remain vigilant to understand what they did on these systems. Memory can give you a quick shot at their actions. Finally, sometimes it is the legitimate user of a machine who misueses IT assets for criminal actions. There are several artifacts in memory that allow investigators to get a better idea about what users have done most recently on commputers. It includes the extraction of encryption keys and even Facebook chat messages. This can be valuable for internal and criminal investigations. We will also focus on how the corresponding volatility plugins work so you will be able to write your own later in the class.

TOPICS: Finding Malware – Injection; Finding Malware – Hooks; DKOM (Direct Kernel Object Manipulation); WinDBG; Artifact Extraction; User Artifacts

SECTION 4: Intrusion Forensics

Memory forensics is a cutting-edge field. That means that many possibilities have not been explored yet. So it makes sense to be able to push the current borders of memory forensics further. Today's enterprise infrastructures heavily rely on containerization. The main representative of that is docker. In this section we will have a shot at docker memory forensics. You will experience how attackers gain access to docker containers firsthand and then you will investigate the breach yourself. As volatility 3 is powerful but still lacks a large number of plugins compared to volatility 2, we will dig into how to write our own psxview plugin for volatility 3. Based on that you will be able to build a plugin for every technique you applied using volshell. Memory is short-lived is what we hear a lot. This is not quite true. First of all, servers keep running for long stretches of time and even than they are rarely switched off but rebooted. Secondly most people do not fully shutdown their machines which also preserves a number of memory artifacts. Finally, there are a few portions of memory that are preserved on the hard drive for indefinite amounts of time. These might make the difference between success and failure in critical investigations. We will investigate page files, hibernation files, and crash dumps. Finally, you can test your knowledge in a scoreboard-style capstone.

TOPICS: Docker Memory Forensics; Custom Volatility Plugins; Page Files and Challenges; Capstone

Who Should Attend

- Incident response team members who regularly respond to complex security incidents/intrusions from APT groups/advanced adversaries and need to know how to detect, investigate, remediate, and recover from compromised systems across an enterprise.
- Threat hunters who are seeking to understand threats more fully and how to learn from them in order to more effectively hunt threats and counter their tradecraft.
- Experienced digital forensic analysts who want to consolidate and expand their understanding of memory and timeline forensics, investigation of technically advanced individuals, incident response tactics, and advanced intrusion investigations.
- Information security professionals who may encounter data breach incidents and intrusions.
- Federal agents and law enforcement professionals who want to master advanced intrusion investigations and incident response, and expand their investigative skills beyond traditional host-based digital forensics.
- Red Team members, penetration testers, and exploit developers who want to learn how their opponents can identify their actions, how common mistakes can compromise operations on remote systems, and how to avoid those mistakes. This course covers remote system forensics and data collection techniques that can be easily integrated into post-exploit operating procedures and exploit- testing batteries.
- SANS FOR508, FOR608 and FOR610 graduates looking to take their skills to the next level.