GUIDEM

DIGITAL FORENSICS MEMORY ANALYSIS

LEVEL UP!

- Perform data acquisition in a forensically sound manner
- Learn how to analyze and perform disk forensics
- Analyze advanced windows event logs in a high scale environment
- Perform memory dump and learn how to dissect IOC and critical information via memory forensics
- Learn the different Windows artifacts and usage of it
- Ransomware analysis and dynamic investigation of malware
- Acquire timeline analysis & writing an incident response report

Authors: Renzon Cruz, Mark Christian Secretario
& Shekinah Ramos

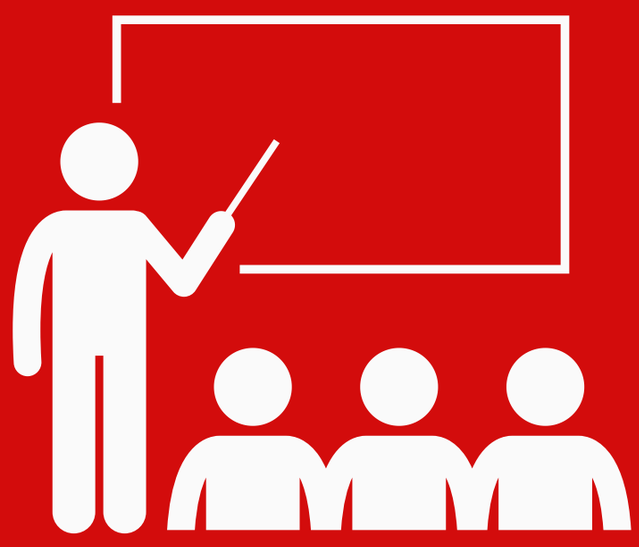
Company Profile

GuideM is a top specialized training provider that delivers real-world approaches in both Offensive (Red) and Defensive (Blue) disciplines of Cybersecurity in the Philippines. We provide professional training and services wherein we take pride in producing world-class quality comprehensive, highly technical, and purely hands-on courses.

OUR INSTRUCTORS

- Seasoned Industry Professionals
- Several years of Experience
- Well known in the industry

OUR COURSES



- Hands-on exercises
- Real-world use cases
- Quality discussion
- Final Challenge (CTF)

GuideM Training courses are intensively for security practitioners to gain real-world hands on knowledge which aim to equip useful skills and practical knowledge that is up to date.

GUIDEM

Our Founder

Mark Christian Secretario, also known as Ian, is a highly experienced cybersecurity professional and the esteemed founder of GuideM. Beyond his technical expertise, He plays a pivotal role in leading GuideM's training and consulting services, offering Security Assessments, VAPT, Red Team, Purple Team, and cybersecurity advisory.

Ian is also responsible for the implementation of a cutting-edge learning platform, keeping GuideM at the forefront of technological advancements. He is actively involved in the company and client's growth, personally teaching and developing both offensive and defensive cybersecurity courses, solidifying GuideM's reputation as a trusted authority in the field. He also guides clients in vetting potential employees from the talent pool and oversees immersive learning events, and customized in-house training. Additionally, Ian is working closely mentoring and guiding the next generation of cybersecurity professionals.

GUIDEM

Course Overview

Cybercrime has quickly risen and is a critical challenge in the cybersecurity industry. Our course will impact IT Security specialists who want to dig deep into digital forensics, data acquisition, incident response, and memory analysis. We will forensically examine digital evidence throughout the training and analyze it to get relevant artifacts to develop an incident hypothesis.

This course will teach you how to identify and respond to threats and information security incidents and develop critical thinking skills to solve computer crime in a forensically sound manner.

Best of all, students will learn a detailed description of how this course can be applied within the laboratory environment and best practice recommendations to perform computer forensics in an enterprise environment.

GUIDEM

Course Structure

This training course presents comprehensive digital forensics concepts as well as memory analysis capabilities that you can leverage in your current work or future career. Our topics included in this boot camp were chosen efficiently based on the market's current demand when looking for a rockstar forensic analyst or digital forensics engineer. This course aims to strengthen your defensive and investigation mindset to deeply analyze huge sets of data; In the end, find and connect all the dots to uncover cybersecurity incidents and attacks.

Learn Digital Forensics based on real-world scenarios and use-cases.

Training Highlights

- 25+ Hand-on Lab Activities
- 600+ Presentation Slides
- 2 custom VMs
- DFMA-WinForensics VM with multiple tools & scripts
- SIFT VM to practice digital forensics and memory analysis
- 5 Hrs of Final Forensics Investigation challenge (CTF)
- GuideM Certification Exam:
  Certified Digital Forensics Analyst (GCDFA)

GUIDEM

Course Author

RENZON CRUZ | @r3nzsec

GDAT | GNFA | GCFA | GCFE | GCIH | eCIR | eCTHP | eCDFP | eJPT | MCS | MCP | ITIL

Principal Consultant, DFIR at Unit 42, Palo Alto Networks | Co-Founder of GuideM

- 10 yrs. of professional experience
- Part of National Security - GCC
- Course Author / Lead Instructor

Specialties & Focus Area:

- SOC & Threat Hunting
- Incident Response
- Digital Forensics
- Malware Analysis
- Adversary Simulation

Speakership:

- BSides London 2019
- BSides Vancouver 2019
- BSides Doha 2020
- ROOTCON PH 2020
- NorthSec Canada 2021
- DEFCON BTV 2021

Certifications:

- GIAC Defending Advanced Threats
- GIAC Certified Forensics Analyst
- GIAC Network Forensics Analyst
- GIAC Certified Forensics Examiner
- GIAC Certified Incident Handler
- eLearnSecurity Threat Hunting Professional
- eLearnSecurity Certified Incident Responder
- eLearnSecurity Digital Forensics Professional
- eLearnSecurity Junior Penetration Tester

GUIDEM

Course Author

MARK CHRISTIAN SECRETARIO | @iansecretario_

Red Team Consultant / Penetration Tester

11+ years in Information Technology

- Malware Development & Purple Team Practitioner
- Freelance & Independent Consultant

Founder and Lead Instructor

- Cybersecurity Training & Services Provider

Hackstreetboys Member

- All Filipino CTF Team

Specialties & Focus Area:

- Red Team/Offensive Security
- Purple Team/Adversary Simulation
- Security Research & Exploit Development
- Evasion and Malware development

Certifications:

- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Enterprise Vulnerability Assessor (GEVA)
- GIAC Exploit Researcher & Advanced Penetration Tester (GXPN)
- GIAC Web Application Penetration Tester (GWAPT)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional(OSCP)
- Certified Red Team Professional (CRTP)
- Certified Red Team Expert (CRTE)
- Certified Red Team Operator(CRTO)
- Certified Red Team Master(CRTM)
- Certified Red Team Lead(CRTL)
- Certified Azure Red Team Professional (CARTP)
- Red Team Operator Level 1 – Rastalabs (Hackthebox)
- Red Team Operator Level 2 – Cybernetics (Hackthebox)
- Red Team Operator Level 3 – APT Labs(Hackthebox)
- Elearnsecurity Exploit Development Professional(eCXD)
- Elearnsecurity Certified Penetration Testing Extreme(eCPTXv2)
- eLearnSecurity Web Application Penetration Tester Expert (eWPTX)
- eLearnSecurity Web ApplicationPenetration Tester (eWPT)
- Pentester Academy Certified Enterprise Specialist (PACES)
- Certified Red Team Professional (Cyberwarfare)
- Certified Red Team Analyst (CyberWarfare)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Network Associate (CCNA)
- CCNA Cyber OPS

GUIDEM

Authors

SHEKINAH RAMOS | @shk1b0i

GCFE | GMON | eCIR | CySA+ | Security+ | CCNP

Co-Founder of GuideM | Administrator

- DFIR/Security Analyst
- Course Author for DFMA

Specialties & Focus Area:

- Digital Forensics
- Incident Response
- Cyber Defense
- Security Operations
- Network Security

Certifications:

- GIAC Certified Forensic Examiner
- GIAC Continuous Monitoring Certification
- eLearnSecurity Certified Incident Responder
- CompTIA Cybersecurity Analyst
- CompTIA Security+
- Cisco Certified Network Professional
- Cisco Certified CyperOps Associate
- Cisco Certified Network Associate
  - Security

GUIDEM

Course Information

System Requirements

- Core i5/Ryzen 5 or greater
- 8GB RAM minimum
- 100GB free storage
- Installed Virtualization software such as VMware Workstation or Fusion

Target Audience

This course is for you if you want to improve your skills in terms of Investigation and Forensic analysis aside from doing the usual threat monitoring.

Blue Team

- Aspiring Digital Forensics & Incident Response
- Career shifters such as Software Engineer, HelpDesk, Network Engineer, System Administrator.
- IT Professionals with a minimum of 1-2 yrs of related experience

Red Team

- Penetration Tester who wants to know how exploits leave artifacts behind and how an investigation works, and to improve their evasion techniques

GUIDEM

Module 1

Introduction to Digital Forensics & Core Concepts

This module is an introductory section to discuss the digital forensics concept and methodology. We will also discuss the life of a forensic examiner and the possible roles once you know digital forensics. We will also showcase the standard tools and their usage to automate the analysis and investigation. This will also include real-world use cases and the challenges we usually encounter as forensics examiners.

Module Highlights & Key Learning

- Introduction to Digital Forensics
- Role of DFMA to your Career
- Challenges of Digital Forensics World
- The Day in the Life of a DFIR Principal Consultant
- Types of Evidence and Data Sources
- Image Mounting
- Tools for Triage Imaging
- Tools for Memory Dumping
- Triage vs Full Disk Image
- Finding Goodness Using Triage Data
- Real-world Use Cases

GUIDEM

Module 2

Windows Registry, Browser Artifacts & File System Forensics

In this module, you will learn how to interact with the lower levels of files and disks. You will also understand the file structure and learn the various file types. You will also be shown how to analyze NTFS file system structures and apply file carving techniques to retrieve previously removed data. File metadata will be discussed along with the data recovery process and tools. We will also dig dive into the world of Windows registries and how this can be very useful in your forensic investigation. As well as forensicating browser artifacts of your choice and the key artifacts of it.

Module Highlights & Key Learning

- Introduction to Windows registries
- SAM, SYSTEM, SOFTWARE, and NTUSER.DAT hives
- Top 10 Windows Registries for Forensics Examiners
- Investigating Browser Artifacts
- Basic of the File System in Windows
- Recovering Deleted/Unallocated Files
- Master File Table, USNJrnl & $J Analysis
- Anti-Forensics & Detection

GUIDEM

Module 3

Investigating Windows Artifacts & Intrusion Analysis

We all know how important the Windows event logs are in our investigation, so we extend our research on the most uncommon event logs that you may not know. Still, we are critical to forensic examiners. We will also introduce you to multiple Windows artifacts such as Prefetch, Shellbags, Recent Files, Amcache, Shimcache, SRUM, etc. We will look into a different aspect of open-source tools for parsing and investigation.

Module Highlights & Key Learning

- Advances Windows Event Logs Analysis
- Introduction to Windows artifacts
- Artifacts of Execution & Analysis
- Artifacts of File Access & Analysis
- Artifacts of Account usage & Analysis
- Artifacts of Data Exfiltration, File Download & Analysis
- USB Forensics & Analysis
- Parsing Windows Artifacts
- Open-Source Tools for Parsing and Investigation

GUIDEM

Module 4

Introduction to Memory Forensics & Timeline Analysis

We will start our day by acquiring various memory dumps using a variety of tools. We will start analyzing the memory dump by identifying rogue processes, analyzing the process objects, extracting the suspicious files, drivers, and objects, and also identifying some hooking and detection mechanisms via memory. We will also discuss the benefit of performing timeline analysis for every forensic or incident response report where you will see all the suspected events based on the timeline to easily present to the board and C-level within your company.

Module Highlights & Key Learning

- Acquiring Memory Dump (Windows/Linux/Mac/Cloud)
- Memory Forensics: Identify Rogue Process
- Memory Forensics: Analyzing Process Objects
- Memory Forensics: Extracting Processes, Drivers & Objects
- Memory Forensics: Hooking & Detection
- Memory Forensics: Network Artifacts
- Memory Forensics: Code Injection
- Timeline Analysis
- Super Timeline Creation

GUIDEM

Module 5

Common Hacking Techniques, Forensic Analysis & Use Cases

On your last day, we will discuss multiple use cases that we personally encounter on different engagements by solving common incidents such as ransomware, web shell attack, living off the land binaries, and supply chain attack methodologies. We'll tackle the do's and dont's on writing a forensic report while maintaining the technical aspect of the incident. The best way to test our knowledge is to put it into a test through hands-on approach, with that being said, we will have our CTF challenge during the last day of the training where you will apply all the knowledge you've earned from day 1 - day 5 into a forensics style CTF.

Module Highlights & Key Learning

- Investigating Living Off the Land Binaries
- Introduction to Cobalt Strike & Technical Analysis
- Investigation of well-known attacks: Ransomware, WebShell, PowerShell, & Supply Chain Attack Methodologies
- Writing a forensic report/post-incident report
- CTF - Forensics Style
    - (5 hrs full of challenges)

GUIDEM

Contact Us

training@guidem.ph

facebook.com/guidemtraining

linkedin.com/company/guidemtraining

twitter.com/guidemtraining

instagram.com/guidemtraining

GUIDEM