Postgraduate Certificate

Malware Analysis and Development

tech technological university

tech universidad tecnológica

Postgraduate Certificate
Malware Analysis and Development

- Modality: **online**
- Duration: **6 weeks**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/in/information-technology/postgraduate-certificate/malware-analysis-development

Index

01

Introduction

In a digital context where business assets are critically dependent on cyber security, the constant threat of malware represents a significant challenge. In this regard, the proliferation of malicious attacks highlights the urgency of having highly specialized professionals in this area. In this sense, the curriculum addresses the prevailing need for experts who not only understand the complexity of digital threats, but can also design proactive strategies for their detection and mitigation. Graduates will learn essential tools for safeguarding the integrity of systems in an increasingly digitized business environment. With the flexibility of the 100% online modality, this Postgraduate Certificate guarantees the accessibility and continuous updating necessary to face the changing challenges of cyberspace.

Become a Malware expert with innovative dynamic analysis techniques thanks to this exclusive 100% online program"

In today's cybersecurity landscape, the sophistication of cyber threats has reached unprecedented levels, generating a growing demand for professionals specialized in Malware Analysis and Development. The constant evolution of malicious tactics demands an equally dynamic response from cybersecurity experts. In this context, the present TECH university program emerges as a comprehensive solution to address these needs. Designed to provide students with advanced knowledge, the curriculum ranges from a thorough understanding of the nature of malware to the evaluation of anti-malware tools. This comprehensive approach prepares professionals to deal with current and future threats.

The TECH Malware Analysis and Development program syllabus is a robust compendium of knowledge covering various dimensions of the malware world. Graduates will explore in depth the various forms and targets of malware, acquiring advanced knowledge of its nature, functionality and behavior. The program delves into forensic analysis applied to malware, providing students with the skills necessary to identify indicators of compromise (IoC) and attack patterns, crucial for early detection and effective response to security incidents. In addition, the course focuses on the development of specific skills to evaluate and select anti-malware security tools. Students will learn to discern the effectiveness of these tools and their adaptability to particular environments, which is essential in implementing effective defense strategies.

With an innovative and adaptable approach, this university program is presented as a unique program proposal. The 100% online modality and Relearning methodology guarantee a flexible and efficient educational experience, allowing professionals to advance their career without interruption and continuously adapt to the changing demands of the cybersecurity field.

This **Postgraduate Certificate in Malware Analysis and Development** contains the most complete and up-to-date program on the market. The most important features include:

- The development of case studies presented by experts in Malware Analysis and Development
- The graphic, schematic and practical contents with which it is conceived provide cutting- Therapeutics and practical information on those disciplines that are essential for professional practice
- Practical exercises where the self-assessment process can be carried out to improve learning
- Its special emphasis on innovative methodologies
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

You will master call analysis with API monkeys in just 6 weeks of the best online program"

You will learn how to generate Shellcode at the world's top-rated university according to the Trustpilot platform (4.9/5)"

You will have access to a learning system based on repetition, with natural and progressive teaching throughout the entire syllabus.

You will deepen your understanding of Strings obfuscation. Give your career the boost it needs!.

The program includes in its teaching staff professionals from the sector who bring to this program the experience of their work, as well as recognized specialists from leading societies and prestigious universities.

The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive education programmed to learn in real situations.

This program is designed around Problem-Based Learning, whereby the professional must try to solve the different professional practice situations that arise during the academic year For this purpose, the students will be assisted by an innovative interactive video system created by renowned and experienced experts.

02

Objectives

The main objective of this curriculum is to enable graduates to master advanced knowledge about the nature, functionality and behavior of malware. Throughout the program, students will delve into the various forms and targets of malware, enabling them to analyze and develop effective defensive strategies in the cybersecurity arena. In addition, this comprehensive approach seeks to specialize professionals capable of meeting the emerging challenges in the detection, analysis and mitigation of malware threats in complex digital environments. In addition, the use of a 100% online methodology makes learning more flexible, allowing access at any time and place.

You will achieve your objectives thanks to TECH's didactic tools, including explanatory videos and interactive summaries"

General Objectives

- Acquire advanced skills in penetration testing and Red Team simulations, addressing the identification and exploitation of vulnerabilities in systems and networks
- Develop leadership skills to coordinate teams specialized in offensive cybersecurity, optimizing the execution of Pentesting and Red Team projects
- Develop skills in the analysis and development of malware, understanding its functionality and applying defensive and educational strategies
- Refine communication skills by preparing detailed technical and executive reports, presenting findings effectively to technical and executive audiences
- Promote an ethical and responsible practice in the field of cybersecurity, considering ethical and legal principles in all activities

Do you want to experience a quality leap in your career? With TECH you will acquire skills in forensic analysis applied to malware"

Specific Objectives

- Acquire advanced knowledge of the nature, functionality and behavior of malware, understanding its various forms and targets
- Develop skills in forensic analysis applied to malware, enabling the identification of indicators of compromise (IoC) and attack patterns
- Learn strategies for effective malware detection and prevention, including the deployment of advanced security solutions
- Familiarize the student with the development of malware for educational and defensive purposes, allowing a deep understanding of the tactics used by attackers
- Promote ethical and legal practices in malware analysis and development, ensuring integrity and accountability in all activities
- Apply theoretical knowledge in simulated environments, participate in hands-on exercises to understand and counter malicious attacks
- Develop skills to evaluate and select anti-malware security tools, considering their effectiveness and adaptability to specific environments
- Learn how to implement effective mitigation against malicious threats, reducing the impact and spread of malware on systems and networks
- Foster effective collaboration with security teams, integrating strategies and efforts to protect against malware threats

03

Course Management

The program in Malware Analysis and Development has an exceptionally qualified faculty. For this purpose, TECH has selected experts with extensive experience and recognized prestige in leading companies in the cybersecurity sector. This faculty, composed of leading professionals, brings not only their practical experience in malware analysis and development, but also their commitment to the learning of future specialists, guaranteeing an updated education aligned with the current demands and challenges of the cybersecurity field.

Get updated in the configuration of virtual machines and snapshots from the best experts in the field. Launch your career with TECH!"

Management

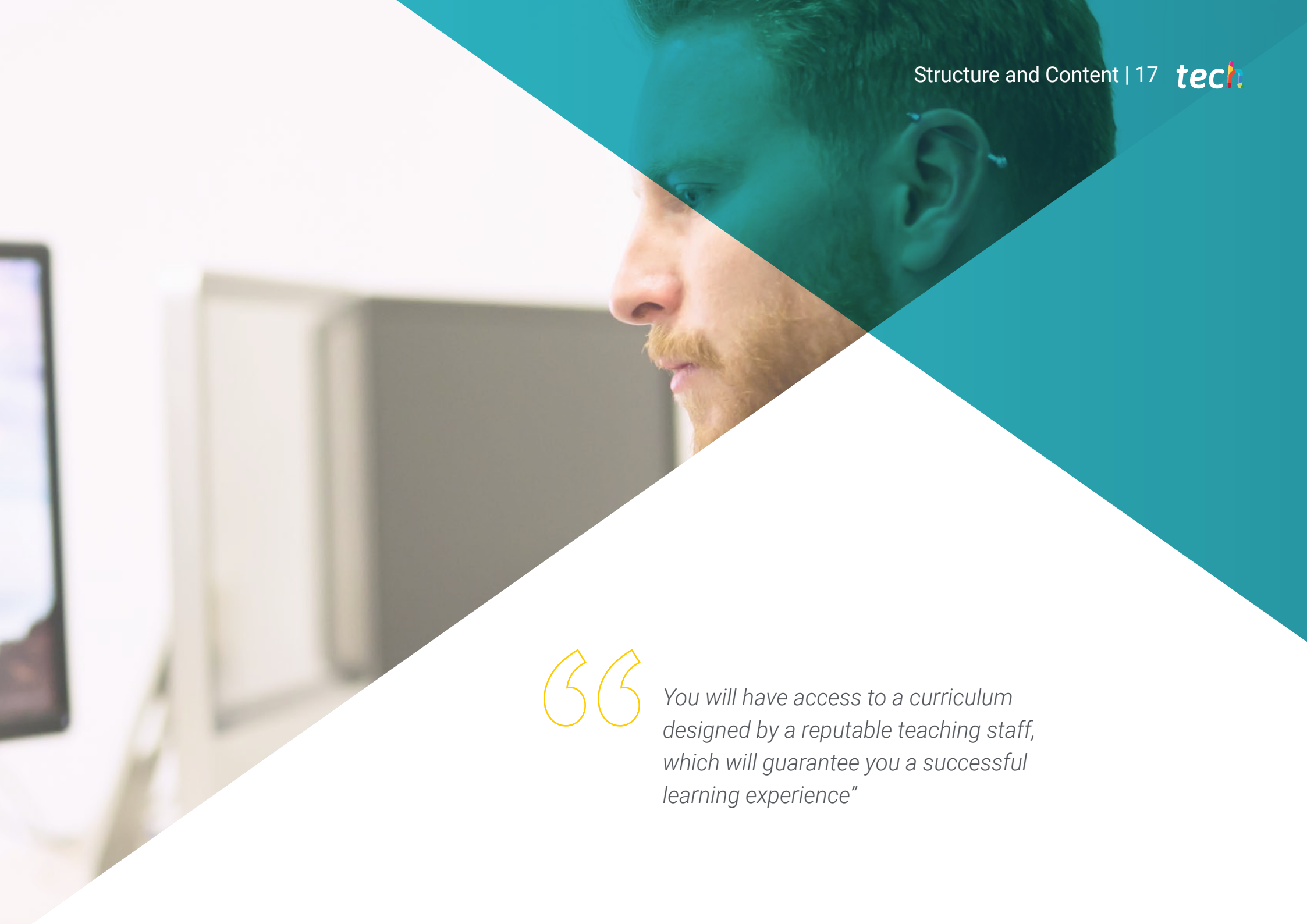
Mr. Carlos Gómez Pintado

- Manager of Cybersecurity and Network Team Cipherbit in Oesía Group
- Manager *Advisor* & *Investor* at Wesson App
- Graduate in Software Engineering and Information Society Technologies, Universidad Politécnica de Madrid
- Collaboration with educational institutions for the development of Higher Level Training Cycles in cybersecurity

04

Structure and Content

This university program will provide students with a deep dive into the world of malware, focusing on its development for educational and defensive purposes. Throughout the course, graduates will address the complexities of malware, allowing a detailed understanding of the tactics employed by attackers. In this regard, the balanced approach of the curriculum not only fosters the acquisition of advanced knowledge in malware analysis, but also trains students to develop essential defensive strategies in the field of cybersecurity.



You will have access to a curriculum designed by a reputable teaching staff, which will guarantee you a successful learning experience"

Module 1. Malware Analysis and Development

1.1. Malware Analysis and Development
- 1.1.1. History and Evolution of Malware
- 1.1.2. Classification and Types of Malware
- 1.1.3. Malware Analysis
- 1.1.4. Malware Development

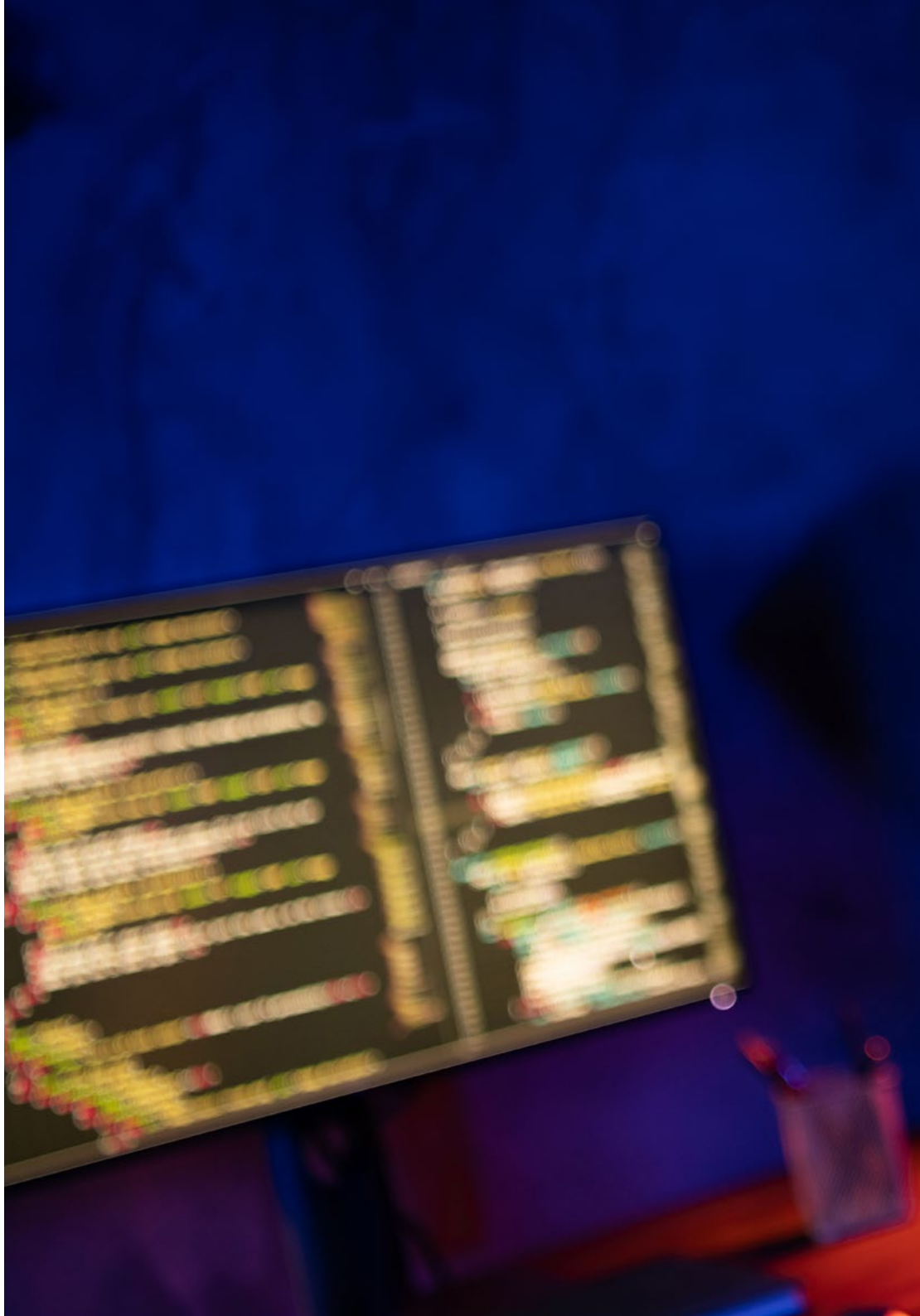
1.2. Preparing the Environment
- 1.2.1. Configuration of Virtual Machines and Snapshots
- 1.2.2. Malware Analysis Tools
- 1.2.3. Malware Development Tools

1.3. Windows Basics
- 1.3.1. PE file format (Portable Executable)
- 1.3.2. Processes and Threads
- 1.3.3. File System and Registry
- 1.3.4. Windows Defender

1.4. Basic Malware Techniques
- 1.4.1. Shellcode Generation
- 1.4.2. Execution of Shellcode on Disk
- 1.4.3. Disk vs Memory
- 1.4.4. Execution of Shellcode in Memory

1.5. Intermediate Malware Techniques
- 1.5.1. Persistence in Windows
- 1.5.2. Home Folder
- 1.5.3. Registration Keys
- 1.5.4. Screensaver

1.6. Advanced Malware Techniques
- 1.6.1. Shellcode Encryption (XOR)
- 1.6.2. Shellcode Encryption (RSA)
- 1.6.3. String Obfuscation
- 1.6.4. Process Injection



1.7. Static Malware Analysis
- 1.7.1. Analyzing Packers with DIE (Detect It Easy)
- 1.7.2. Analyzing Sections with PE-Bear
- 1.7.3. Decompilation with Ghidra

1.8. Dynamic Malware Analysis
- 1.8.1. Observing Behavior with Process Hacker
- 1.8.2. Analyzing Calls with API Monitor
- 1.8.3. Analyzing Registry Changes with Regshot
- 1.8.4. Observing Network Requests with TCPView

1.9. Analysis in .NET
- 1.9.1. Introduction to .NET
- 1.9.2. Decompiling with dnSpy
- 1.9.3. Debugging with dnSpy

1.10. Analyzing Real Malware
- 1.10.1. Preparing the Environment
- 1.10.2. Static Malware Analysis
- 1.10.3. Dynamic Malware Analysis
- 1.10.4. YARA Rule Creation

Don't miss the opportunity to boost your career through this innovative program"

05

Methodology

This academic program offers students a different way of learning. Our methodology uses a cyclical learning approach: **Relearning.**

This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

Discover Relearning, a system that abandons conventional linear learning, to take you through cyclical teaching systems: a way of learning that has proven to be extremely effective, especially in subjects that require memorization"

Case Study to contextualize all content

Our program offers a revolutionary approach to developing skills and knowledge. Our goal is to strengthen skills in a changing, competitive, and highly demanding environment.

At TECH, you will experience a learning methodology that is shaking the foundations of traditional universities around the world"

You will have access to a learning system based on repetition, with natural and progressive teaching throughout the entire syllabus.

The student will learn to solve complex situations in real business environments through collaborative activities and real cases.

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch, which presents the most demanding challenges and decisions in this field, both nationally and internationally. This methodology promotes personal and professional growth, representing a significant step towards success. The case method, a technique that lays the foundation for this content, ensures that the most current economic, social and professional reality is taken into account.

> *Our program prepares you to face new challenges in uncertain environments and achieve success in your career"*

The case method has been the most widely used learning system among the world's leading Information Technology schools for as long as they have existed. The case method was developed in 1912 so that law students would not only learn the law based on theoretical content. It consisted of presenting students with real-life, complex situations for them to make informed decisions and value judgments on how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue and defend their ideas and decisions.

Relearning Methodology

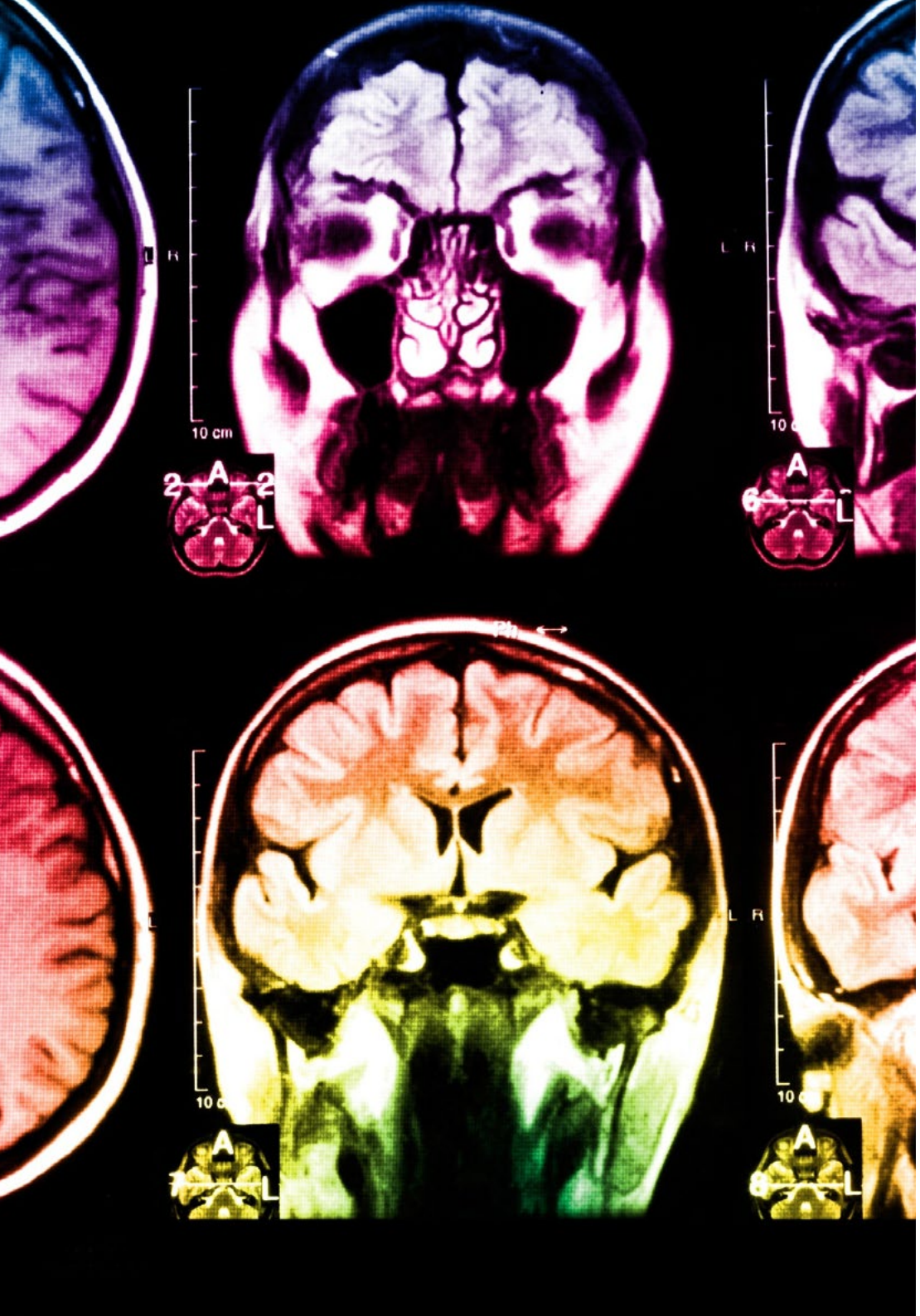
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

We enhance the Case Study with the best 100% online teaching method: Relearning.

In 2019, we obtained the best learning results of all online universities in the world.

At TECH you will learn using a cutting-edge methodology designed to train the executives of the future. This method, at the forefront of international teaching, is called Relearning.

Our university is the only one in the world authorized to employ this successful method. In 2019, we managed to improve our students' overall satisfaction levels (teaching quality, quality of materials, course structure, objectives...) based on the best online university indicators.



In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. This methodology has trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, genetics, surgery, international law, management skills, sports science, philosophy, law, engineering, journalism, history, and financial markets and instruments. All this in a highly demanding environment, where the students have a strong socio-economic profile and an average age of 43.5 years.

Relearning will allow you to learn with less effort and better performance, involving you more in your training, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation for success.

From the latest scientific evidence in the field of neuroscience, not only do we know how to organize information, ideas, images and memories, but we know that the place and context where we have learned something is fundamental for us to be able to remember it and store it in the hippocampus, to retain it in our long-term memory.

In this way, and in what is called neurocognitive context-dependent e-learning, the different elements in our program are connected to the context where the individual carries out their professional activity.

This program offers the best educational material, prepared with professionals in mind:

Study Material

All teaching material is produced by the specialists who teach the course, specifically for the course, so that the teaching content is highly specific and precise.

These contents are then applied to the audiovisual format, to create the TECH online working method. All this, with the latest techniques that offer high quality pieces in each and every one of the materials that are made available to the student.

Classes

There is scientific evidence suggesting that observing third-party experts can be useful.

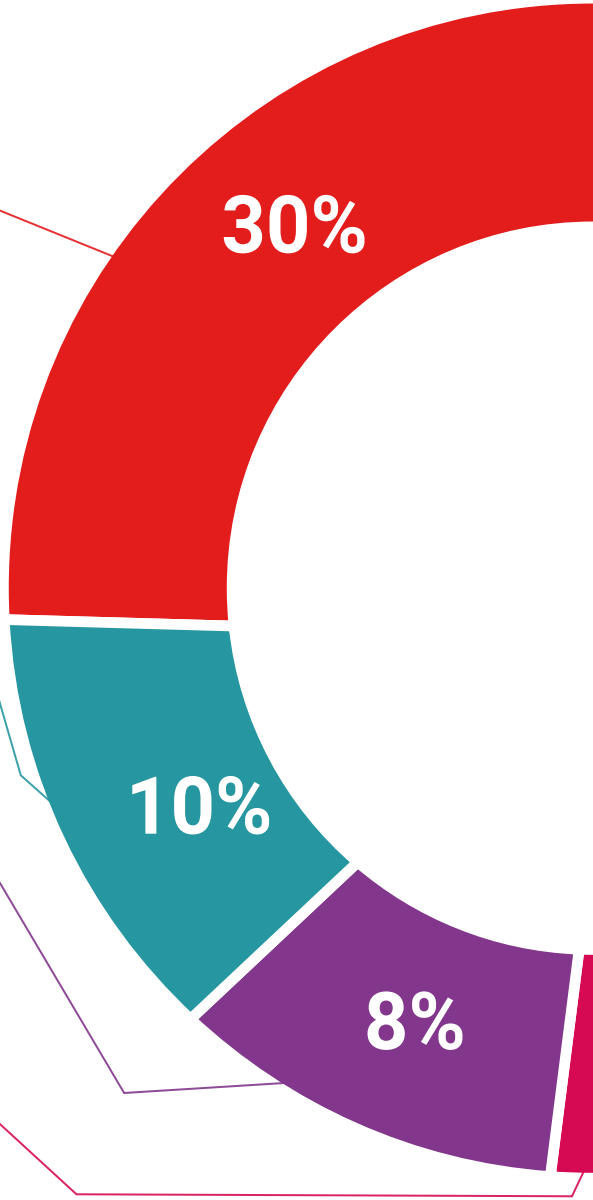
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

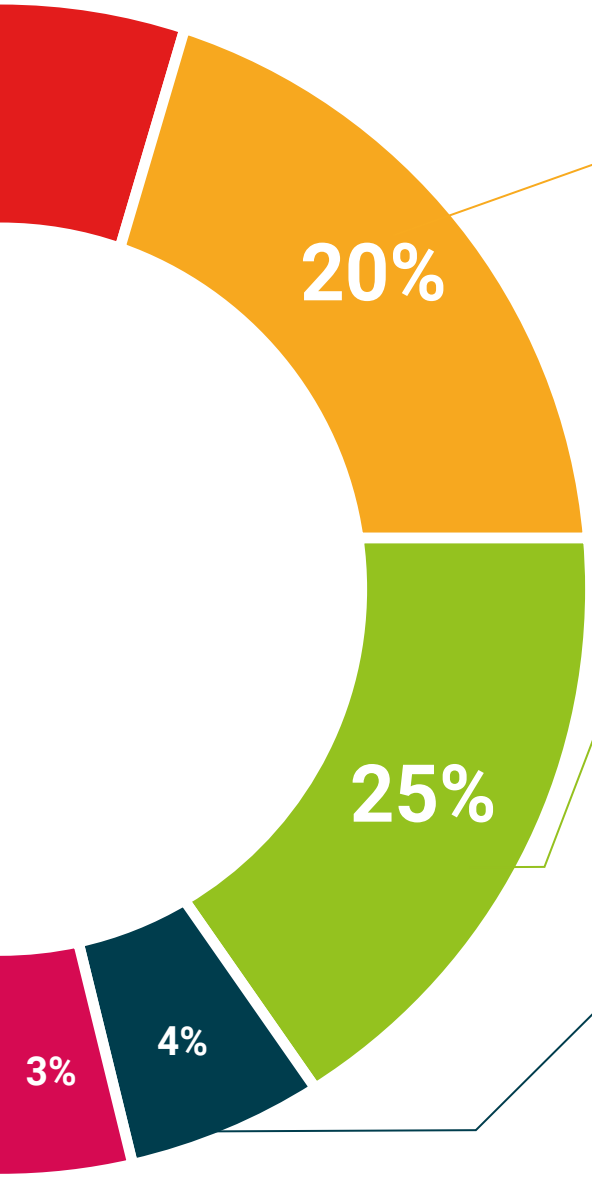
Practising Skills and Abilities

They will carry out activities to develop specific skills and abilities in each subject area. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop in the context of the globalization that we are experiencing.

Additional Reading

Recent articles, consensus documents and international guidelines, among others. In TECH's virtual library, students will have access to everything they need to complete their course.





Case Studies

Students will complete a selection of the best case studies chosen specifically for this program. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Interactive Summaries

The TECH team presents the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

Testing & Retesting

We periodically evaluate and re-evaluate students' knowledge throughout the program, through assessment and self-assessment activities and exercises, so that they can see how they are achieving their goals.

06

Certificate

The Postgraduate Certificate in Malware Analysis and Development guarantees students, in addition to the most rigorous and up-to-date education, access to a Postgraduate Certificate issued by TECH Technological University.

Successfully complete this program and receive your university qualification without having to travel or fill out laborious paperwork"

This **Postgraduate Certificate in Malware Analysis and Development** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Postgraduate Certificate** issued by **TECH Technological University** via tracked delivery*.

The certificate issued by **TECH Technological University** will reflect the qualification obtained in the Postgraduate Certificate, and meets the requirements commonly demanded by labor exchanges, competitive examinations and professional career evaluation committees.

Title: **Postgraduate Certificate in Malware Analysis and Development**

Official Nº of Hours: **150 h.**


tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _____, with identification number _____.

For having passed and accredited the following program

POSTGRADUATE CERTIFICATE

in

Malware Analysis and Development

This is a qualification awarded by this University, equivalent to 150 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates

*Apostille Convention. In the event that the student wishes to have their paper certificate issued with an apostille, TECH EDUCATION will make the necessary arrangements to obtain it, at an additional cost.

tech technological university

Postgraduate Certificate
Malware Analysis and Development

- Modality: **online**
- Duration: **6 weeks**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Postgraduate Certificate

Malware Analysis and Development

tech technological university