

EXP:1 WINDOWS FORENSICS

AIM: To learn about the introduction to windows registry forensics.

The screenshot shows the 'Windows Forensics 1' room completion page on the TryHackMe platform. The room title is 'Windows Forensics 1' with the subtitle 'Introduction to Windows Registry Forensics'. It indicates a duration of 60 minutes and 88,705 views. The page lists 11 tasks, all of which are marked as completed with green checkmarks:

- Task 1: Introduction to Windows Forensics
- Task 2: Windows Registry and Forensics
- Task 3: Accessing registry hives offline
- Task 4: Data Acquisition
- Task 5: Exploring Windows Registry
- Task 6: System Information and System Accounts
- Task 7: Usage or knowledge of files/folders
- Task 8: Evidence of Execution
- Task 9: External Devices/USB device forensics
- Task 10: Hands-on Challenge
- Task 11: Conclusion

At the bottom, there is a recommendation section asking 'How likely are you to recommend this room to others?' with a rating scale from 1 to 10. The 'Submit now' button is visible.

RESULT:

Thus about windows registry forensics has been successfully completed.

EXP :2 VOLATILITY ESSENTIALS

AIM: To learn how to perform memory forensics with volatility

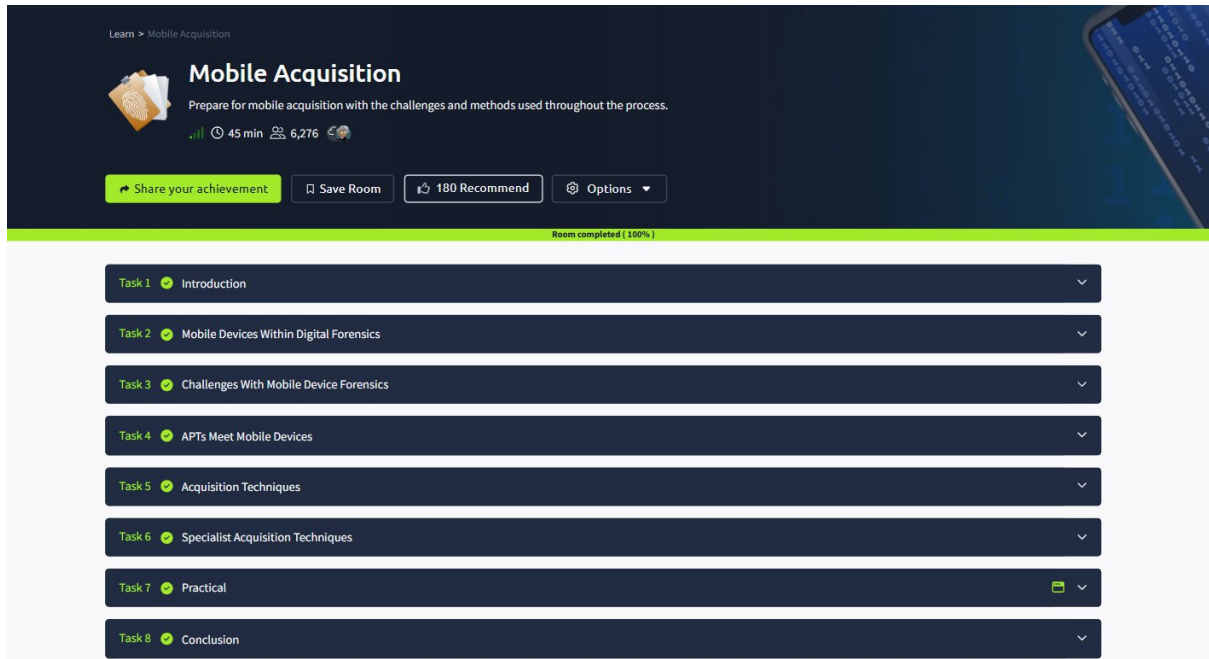
The screenshot shows the 'Volatility Essentials' room completion page on the TryHackMe platform. The top navigation bar includes the TryHackMe logo, 'Dashboard', 'Learn', 'Practice', and 'Compete' tabs, along with a search icon, a notification bell, a 'Go Premium' button, and a user profile icon. The main header area displays the room title 'Volatility Essentials' with a sub-header 'Learn how to perform memory forensics with Volatility!'. Below this, it shows a progress bar, a timer for 60 minutes, and a count of 3,812 participants. Action buttons include 'Share your achievement', 'Save Room', '104 Recommend', and 'Options'. A green banner indicates 'Room completed (100%)'. The main content area lists eight tasks, all marked as completed with green checkmarks: Task 1 Introduction, Task 2 Volatility Overview, Task 3 Memory Acquisition and Analysis, Task 4 Listing Processes and Connections, Task 5 Volatility Hunting and Detection Capabilities, Task 6 Advanced Memory Forensics, Task 7 Practical Investigations, and Task 8 Conclusion. At the bottom, there is a feedback section asking 'How likely are you to recommend this room to others?' with a rating scale from 1 to 10 and a 'Submit now' button.

RESULT:

Thus about memory forensics with volatility has been studied and executed.

EXP:3 MOBILE ACQUISITION

AIM: To prepare for mobile acquisition with the challenges and methods used throughout the process.



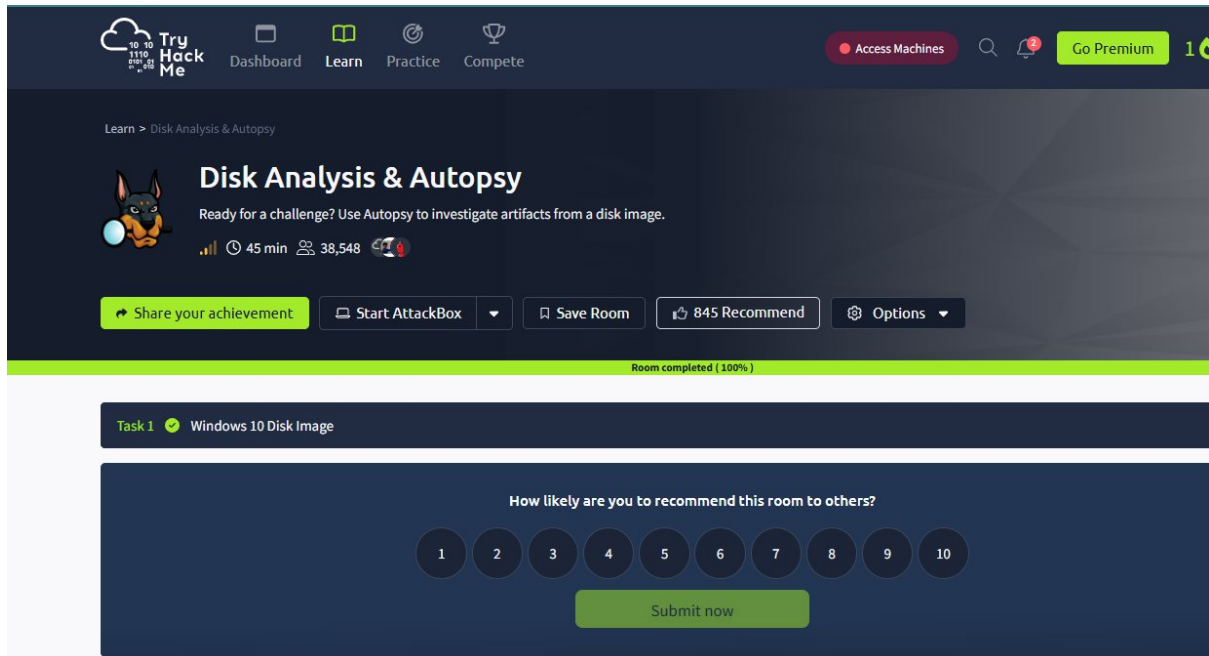
The screenshot displays a course interface for 'Mobile Acquisition'. At the top, it says 'Learn > Mobile Acquisition' and 'Mobile Acquisition'. Below this, a description reads: 'Prepare for mobile acquisition with the challenges and methods used throughout the process.' It also shows a duration of '45 min', a rating of '6,276', and a 'Share your achievement' button. A row of buttons includes 'Save Room', '180 Recommend', and 'Options'. A green progress bar indicates 'Room completed (100%)'. Below this, a list of tasks is shown, each with a green checkmark and a dropdown arrow:

- Task 1 Introduction
- Task 2 Mobile Devices Within Digital Forensics
- Task 3 Challenges With Mobile Device Forensics
- Task 4 APTs Meet Mobile Devices
- Task 5 Acquisition Techniques
- Task 6 Specialist Acquisition Techniques
- Task 7 Practical
- Task 8 Conclusion

RESULT: Hence the mobile acquisition has been studied and successfully executed.

EXP:4 DISK ANALYSIS & AUTOPSY

AIM: To use autopsy to investigate artifacts from a disk image



RESULT:

Hence the disk analysis and forensics in tryhackme has been successfully studied.

EXP:5 INTRO TO COLD SYSTEM FORENSICS

AIM: To study about cold system forensics in tryhackme.

The screenshot shows the completion page for the 'Intro to Cold System Forensics' room on TryHackMe. The header includes the room title, a description, and statistics: 60 min duration, 8,400 participants, and 268 recommendations. A green bar at the top indicates 'Room completed (100%)'. Below this, a list of six tasks is shown, each with a green checkmark indicating completion: Task 1 Introduction, Task 2 Challenges and Opportunities, Task 3 Data Acquisition and Preservation, Task 4 Forensic Tools and Techniques, Task 5 Practical, and Task 6 Conclusion. At the bottom, there is a rating section titled 'How likely are you to recommend this room to others?' with a scale from 1 to 10 and a 'Submit now' button.

Learn > Intro to Cold System Forensics

Intro to Cold System Forensics

A look into the concepts of cold system forensics and how DFIR teams examine offline systems.

60 min 8,400 268 Recommend Options

Share your achievement Save Room

Room completed (100%)

- Task 1 Introduction
- Task 2 Challenges and Opportunities
- Task 3 Data Acquisition and Preservation
- Task 4 Forensic Tools and Techniques
- Task 5 Practical
- Task 6 Conclusion

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Submit now

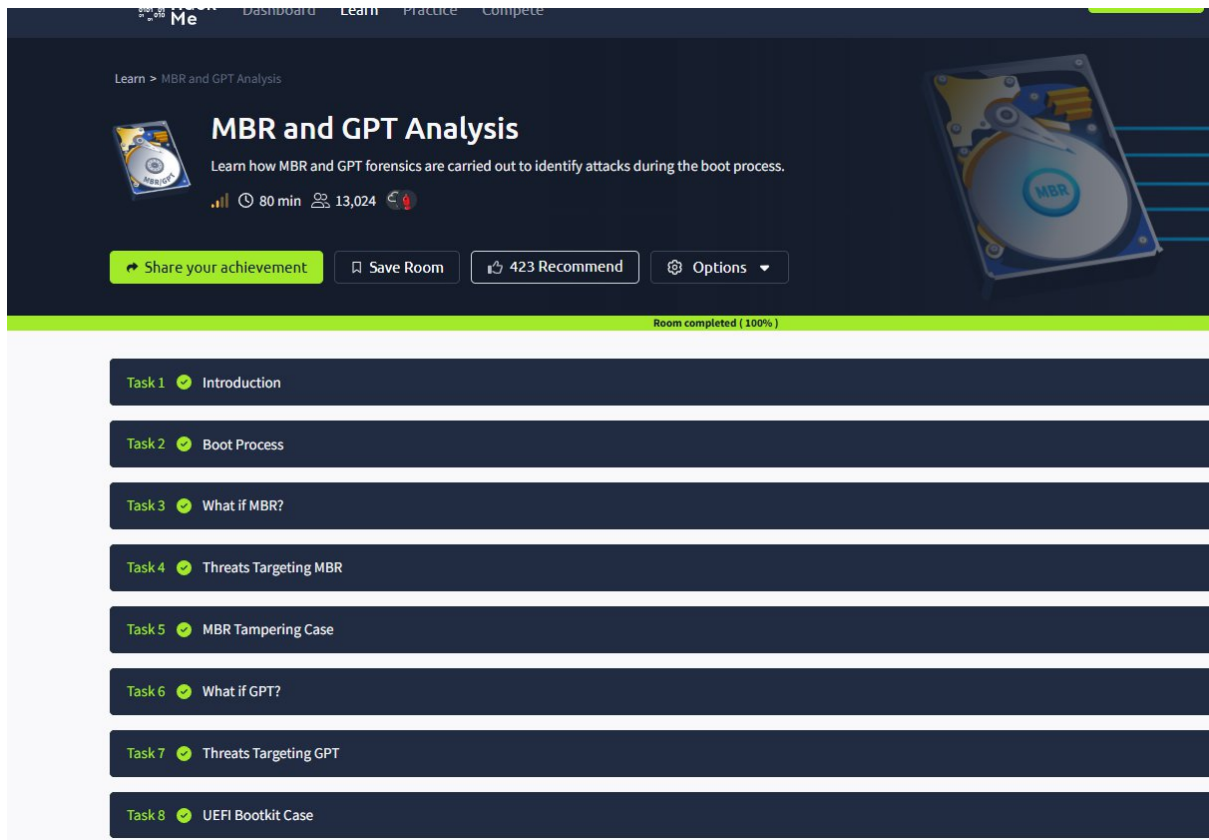
RESULT:

Hence concept of cold system forensics were studied .

EXP:6

MBR AND GPT ANALYSIS

AIM: To learn how MBR and GPT forensics are carried out to identify attacks during the boot process.



The screenshot shows a HackTheBox CTF room interface. At the top, there's a navigation bar with 'Me', 'Dashboard', 'Learn', 'Practice', and 'Complete'. Below this, the room title 'MBR and GPT Analysis' is displayed, along with a description: 'Learn how MBR and GPT forensics are carried out to identify attacks during the boot process.' To the right of the title is a large image of a hard drive with 'MBR' written on it. Below the title, there are statistics: '80 min' for time, '13,024' for users, and '423 Recommend'. There are also buttons for 'Share your achievement', 'Save Room', and 'Options'. A green bar at the bottom of the header indicates 'Room completed (100%)'. Below this, a list of tasks is shown, each with a green checkmark indicating completion:

- Task 1 ✓ Introduction
- Task 2 ✓ Boot Process
- Task 3 ✓ What if MBR?
- Task 4 ✓ Threats Targeting MBR
- Task 5 ✓ MBR Tampering Case
- Task 6 ✓ What if GPT?
- Task 7 ✓ Threats Targeting GPT
- Task 8 ✓ UEFI Bootkit Case

RESULT:

Thus about MBR and GPT forensics have been successfully studied.

EXP :7

FAT32 ANALYSIS

AIM: To examine FAT32 filesystem from a forensic point of view.

The screenshot displays the 'FAT32 Analysis' room interface. At the top, there's a header with a 'FAT32' icon, the title 'FAT32 Analysis', and a subtitle 'Examine the FAT32 filesystem from a forensic point of view.' Below this, a progress bar shows 'Room completed (100%)'. The main content area lists 11 tasks, each with a green checkmark indicating completion. The tasks are: Task 1: Introduction, Task 2: Environment and Setup, Task 3: FAT32: Relevancy in Cyber Security, Task 4: FAT32 Structure: Reserved and FAT Areas, Task 5: FAT32 Structure: Data Area, Task 6: FAT32: Analysis Techniques and Tools, Task 7: T1564.001 Hidden Files and Directories, Task 8: T1070.006 Indicator Removal: Timestamp, Task 9: T1070.004 File Deletion and T1070.009 Clear Persistence, Task 10: Challenge, and Task 11: Conclusion. The interface also includes buttons for 'Share your achievement', 'Save Room', '158 Recommend', and 'Options'.

FAT32 Analysis
Examine the FAT32 filesystem from a forensic point of view.

90 min 5,767 N

Share your achievement Save Room 158 Recommend Options

Room completed (100%)

- Task 1 Introduction
- Task 2 Environment and Setup
- Task 3 FAT32: Relevancy in Cyber Security
- Task 4 FAT32 Structure: Reserved and FAT Areas
- Task 5 FAT32 Structure: Data Area
- Task 6 FAT32: Analysis Techniques and Tools
- Task 7 T1564.001 Hidden Files and Directories
- Task 8 T1070.006 Indicator Removal: Timestamp
- Task 9 T1070.004 File Deletion and T1070.009 Clear Persistence
- Task 10 Challenge
- Task 11 Conclusion

RESULT:

Thus FAT32 Analysis in tryhackme has been successfully studied.

EXP: 8 FORENSIC IMAGING

AIM: To learn the basic concepts of forensic imaging

The screenshot shows the 'Forensic Imaging' room completion page on TryHackMe. The header includes the room title 'Forensic Imaging' with a subtitle 'Learn the basic concepts of forensic imaging.' and statistics: 45 min, 11,596 users, and 290 recommendations. A green bar indicates 'Room completed (100%)'. Below this, a list of tasks is shown, all marked as completed with green checkmarks:

- Task 1: Introduction
- Task 2: Preparation
- Task 3: Creating a Forensic Image
- Task 4: Integrity Checking
- Task 5: Other Types of Imaging
- Task 6: Practical Exercise
- Task 7: Conclusion

At the bottom, there is a recommendation section titled 'How likely are you to recommend this room to others?' with a rating scale from 1 to 10. The 'Submit now' button is visible.

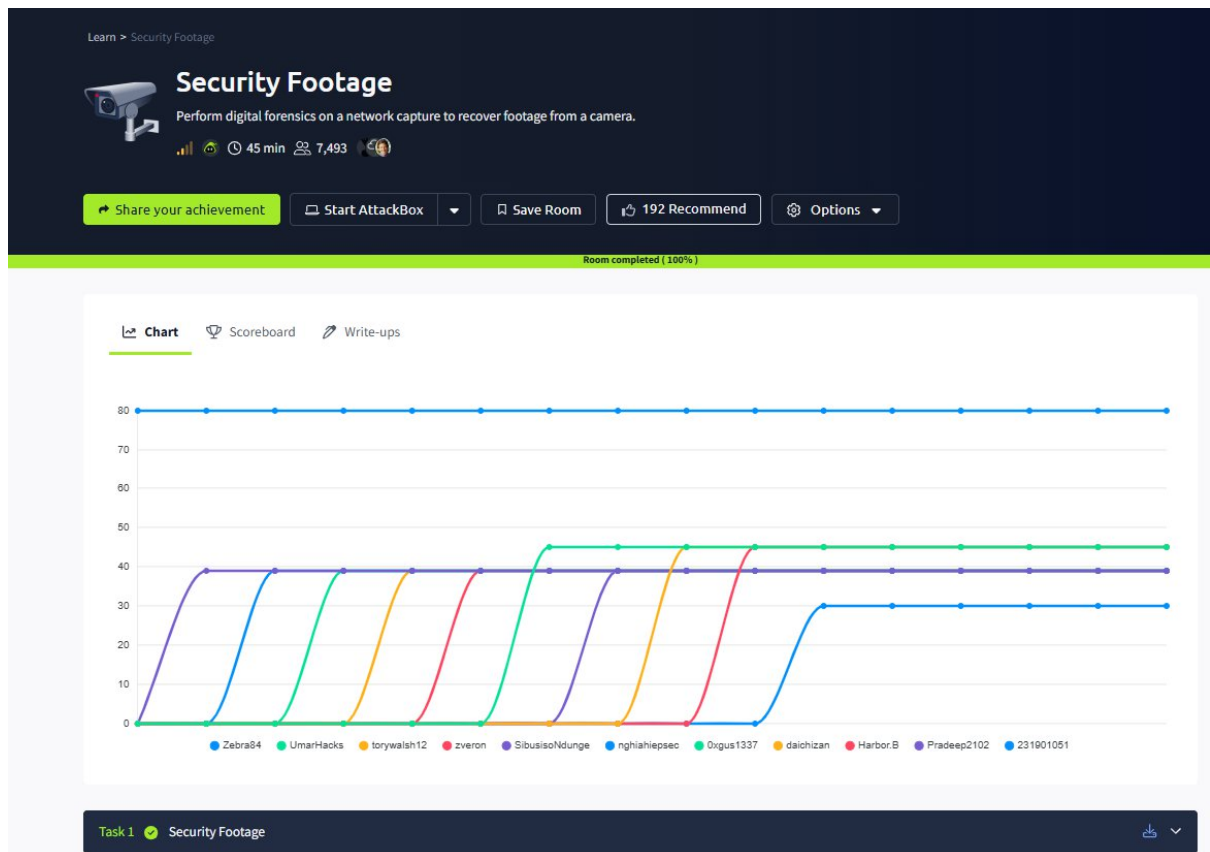
RESULT:

Thus about forensic imaging in tryhackme has been successfully studied.

EXP:9

SECURITY FOOTAGE

AIM: To perform digital forensic on the network capture to recover footage .



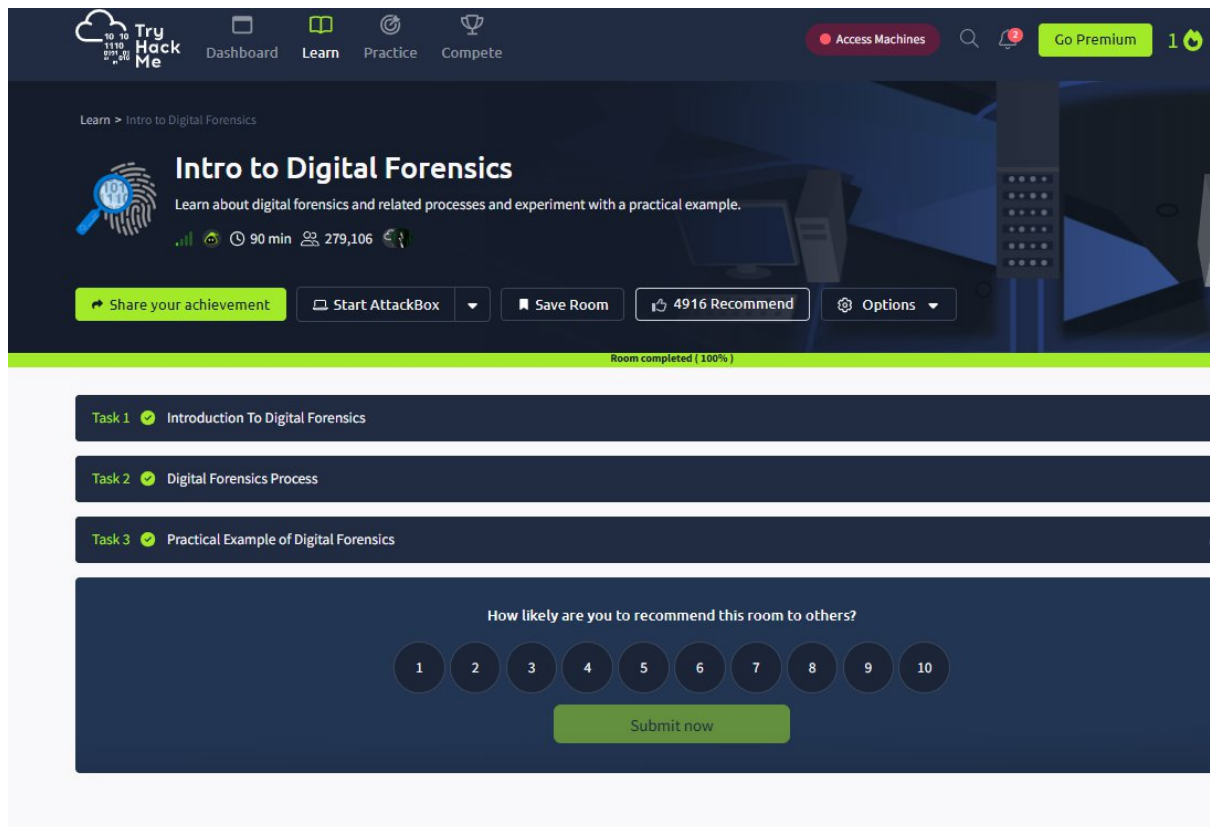
RESULT:

Hence the security footage is studied and practised in tryhackme.

EXP:10

INTRO TO DIGITAL FORENSICS

AIM: To learn about digital forensics and its related processes.



RESULT:

The basic about digital forensics has been successfully completed.

EXP: 11 MACOS FORENSICS:THE BASICS

AIM: To learn the basics to prepare for performing forensics on macos.

The screenshot shows the 'macOS Forensics: The Basics' room completion page on the TryHackMe platform. The page has a dark blue header with navigation links: Dashboard, Learn, Practice, and Compete. A 'Go Premium' button and a user profile icon are on the right. Below the header, the room title 'macOS Forensics: The Basics' is displayed with a subtitle 'Learn the basics to prepare for performing forensics on macOS.' and a small icon of a computer. Below this, a progress bar shows 'Room completed (100%)'. A list of tasks follows, each marked with a green checkmark, indicating completion: Task 1 Introduction, Task 2 A Brief History of macOS, Task 3 HFS+ File System, Task 4 APFS File System, Task 5 macOS Directory Structure and Domains, Task 6 macOS File Formats, Task 7 Challenges in Data Acquisition, Task 8 Mounting APFS Disk Image, and Task 9 Conclusion. At the bottom, there are buttons for 'Share your achievement', 'Save Room', '211 Recommend', and 'Options'.

TryHackMe

Dashboard Learn Practice Compete

Go Premium 1

Learn > macOS Forensics: The Basics

macOS Forensics: The Basics

Learn the basics to prepare for performing forensics on macOS.

90 min 6,895

Share your achievement Save Room 211 Recommend Options

Room completed (100%)

- Task 1 Introduction
- Task 2 A Brief History of macOS
- Task 3 HFS+ File System
- Task 4 APFS File System
- Task 5 macOS Directory Structure and Domains
- Task 6 macOS File Formats
- Task 7 Challenges in Data Acquisition
- Task 8 Mounting APFS Disk Image
- Task 9 Conclusion

RESULT:

Hence basics of macos forensic were successfully studied.

EXP: 12

LINUX SERVER FORENSICS

AIM: To learn about digital forensics artefacts found on linux servers by analysing a compromised server.

The screenshot shows the 'Linux Server Forensics' challenge page on TryHackMe. The header includes the challenge title, a description, and statistics: 75 min, 10,474 attempts, and 472 recommendations. Below the header is a list of 11 tasks, all marked as completed with green checkmarks. The tasks are: Task 1: Deploy the first VM, Task 2: Apache Log Analysis I, Task 3: Web Server Analysis, Task 4: Persistence Mechanisms I, Task 5: User Accounts, Task 6: Deploy the second VM, Task 7: Apache Log Analysis II, Task 8: Persistence Mechanisms II, Task 9: Program Execution History, Task 10: Deploy The Final VM, and Task 11: Persistence Mechanisms III. A green bar at the top of the task list indicates 'Room completed (100%)'.

Linux Server Forensics
Learn about digital forensics artefacts found on Linux servers by analysing a compromised server

75 min 10,474 472 Recommend Options

Share your achievement Start AttackBox Save Room 472 Recommend Options

Room completed (100%)

- Task 1 ✓ Deploy the first VM
- Task 2 ✓ Apache Log Analysis I
- Task 3 ✓ Web Server Analysis
- Task 4 ✓ Persistence Mechanisms I
- Task 5 ✓ User Accounts
- Task 6 ✓ Deploy the second VM
- Task 7 ✓ Apache Log Analysis II
- Task 8 ✓ Persistence Mechanisms II
- Task 9 ✓ Program Execution History
- Task 10 ✓ Deploy The Final VM
- Task 11 ✓ Persistence Mechanisms III

RESULT:

Hence the linux server forensics is studied and successfully executed.