

SHRINIDHI
231901050

EXERCISE - 01

The screenshot shows the 'Intro to Digital Forensics' room completion page on TryHackMe. The top navigation bar includes the TryHackMe logo, links to Dashboard, Learn, Practice, and Compete, and buttons for Access Machines, Go Premium, and a user profile icon. The main header area displays the room title 'Intro to Digital Forensics' with a magnifying glass icon, a description 'Learn about digital forensics and related processes and experiment with a practical example.', and statistics: 90 min, 279,040 views, and 4916 recommendations. Below this are buttons for 'Share your achievement', 'Start AttackBox', 'Save Room', and 'Options'. A green progress bar indicates 'Room completed (100%)'. The task list shows three tasks: 'Task 1 Introduction To Digital Forensics', 'Task 2 Digital Forensics Process', and 'Task 3 Practical Example of Digital Forensics', all marked as completed. The bottom section features a rating prompt 'How likely are you to recommend this room to others?' with a 1-10 scale and a 'Submit now' button.

TryHackMe

Dashboard Learn Practice Compete

Access Machines Go Premium 0

Learn > Intro to Digital Forensics

Intro to Digital Forensics

Learn about digital forensics and related processes and experiment with a practical example.

90 min 279,040 4916 Recommend Options

Share your achievement Start AttackBox Save Room

Room completed (100%)

Task 1 Introduction To Digital Forensics

Task 2 Digital Forensics Process


Task 3 Practical Example of Digital Forensics

How likely are you to recommend this room to others?





1 2 3 4 5 6 7 8 9 10

Submit now


EXERCISE - 02



[Dashboard](#) [Learn](#) [Practice](#) [Compete](#)





[Access Machines](#)   [Go Premium](#)  

[Learn](#) > [Windows Forensics 1](#)




Windows Forensics 1


Introduction to Windows Registry Forensics



  60 min  88,594 


[Share your achievement](#) [Start AttackBox](#) [Save Room](#) [2127 Recommend](#) [Options](#)


Room completed (100%)


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 

How likely are you to recommend this room to others?

1

2

3

4

5

6

7


8

9

10


Submit now

EXERCISE - 03




DashboardLearnPracticeCompete

Go Premium0








Learn > macOS Forensics: The Basics




macOS Forensics: The Basics


Learn the basics to prepare for performing forensics on macOS.



 90 min  6,872 


[Share your achievement](#)[Save Room](#)[210 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

How likely are you to recommend this room to others?

12345678910


Submit now

EXERCISE - 04




DashboardLearnPracticeCompete

Go Premium0



Learn > Volatility Essentials



Volatility Essentials

Learn how to perform memory forensics with Volatility!


60 min3,794

[Share your achievement](#)[Save Room](#)[104 Recommend](#)[Options](#)

Room completed (100%)

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



Task 8 ✓ Conclusion

How likely are you to recommend this room to others?


12345678910

Submit now

EXERCISE - 05





DashboardLearnPracticeCompeteGo Premium0

Learn > Mobile Acquisition




Mobile Acquisition

Prepare for mobile acquisition with the challenges and methods used throughout the process.

  45 min  6,243 


Share your achievementSave Room180 RecommendOptions

Room completed (100%)

 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

▼

How likely are you to recommend this room to others?

1

2

3

4

5

6

7


8

9




10

Submit now


EXERCISE - 06



[Dashboard](#) [Learn](#) [Practice](#) [Compete](#)






[Access Machines](#)   [Go Premium](#) 0 

[Learn](#) > Linux Server Forensics




Linux Server Forensics

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


  75 min  10,447  


[Share your achievement](#) [Start AttackBox](#) [Save Room](#) [471 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

▾

How likely are you to recommend this room to others?

1

2

3

4

5

6

7



8

9


10

Submit now

EXERCISE - 07





DashboardLearnPracticeCompeteAccess MachinesGo Premium0

Learn > Disk Analysis & Autopsy





Disk Analysis & Autopsy


Ready for a challenge? Use Autopsy to investigate artifacts from a disk image.

  45 min  38,511 

Share your achievementStart AttackBoxSave Room844 RecommendOptions

Room completed (100%)

Task 1  Windows 10 Disk Image 100 



How likely are you to recommend this room to others?


12345678910

Submit now




EXERCISE - 08




EXERCISE - 09



[Dashboard](#) [Learn](#) [Practice](#) [Compete](#)





[Go Premium](#) 0 

[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  8,361 


[Share your achievement](#) [Save Room](#) [267 Recommend](#) [Options](#)


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


EXERCISE - 10



[Dashboard](#) [Learn](#) [Practice](#) [Compete](#)





  [Go Premium](#) 0 

[Learn](#) > MBR and GPT Analysis




MBR and GPT Analysis

Learn how MBR and GPT forensics are carried out to identify attacks during the boot process.


  80 min  12,937 

[Share your achievement](#) [Save Room](#) [422 Recommend](#) [Options](#)

Room completed (100%)

 Task 3

✔ What if MBR?



Task 1 ✔ Introduction

Task 2 ✔ Boot Process

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

How likely are you to recommend this room to others?

1

2

3

4

5

6

7



8

9


10

Submit now

EXERCISE - 11





DashboardLearnPracticeCompeteGo Premium0

Learn > FAT32 Analysis




FAT32 Analysis

Examine the FAT32 filesystem from a forensic point of view.

  90 min  5,724  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: Timestomp

▼

 Task 9


T1070.004 File Deletion and T1070.009 Clear Persistence

▼

 Task 10

Challenge

▼

 Task 11

Conclusion

▼

How likely are you to recommend this room to others?

1

2

3

4

5

6

7



8

9


10

Submit now

EXERCISE - 12





DashboardLearnPracticeCompeteAccess MachinesGo Premium0

Learn > Forensic Imaging




Forensic Imaging


Learn the basic concepts of forensic imaging.



  45 min  11,550 


Share your achievementStart AttackBoxSave Room290 RecommendOptions


Room completed (100%)


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

How likely are you to recommend this room to others?

12345678910

Submit now