A ROADMAP

$: whoami

Nishant Grover

Interest: Incident Response, Scripting, threat hunting

@ngrovyer

$: man CHFI

CHFIv8 presents step-by-step procedures, best practices and guidelines to carry out forensic investigation.

Organization: EC Council

Exam Code:– 312-49 (v9)

Basic certificate for Digital forensics

Well known in Indian companies and abroad

Good for Freshers – 3-4 Years of exp

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: man CHFI | more

Vendor Neutral

Cheap: 450 USD (30,000 to 32,000 INR) (latest one: 31546)

Suggested for roles: SOC Analyst, Incident Response, Digital forensics Investigator, Security consultant

EC Council Recommendation: To be done after you have completed CEH

My Recommendation: CEH, Not a requirement

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -h Eligibility

A. Proven experience of 2 years of working in Information Security

- Without Training
- You save 50 USD (total cost 400 USD)
- 100 USD will be non refundable processing fee

B. Attend official CHFI training

C|HFI™ Computer Hacking Forensic INVESTIGATOR

>>> define exam_process(CHFI)

150 Multiple Choice Questions

Exam time: 4 Hours

Can be taken from home

Schedule: Monday – Friday

Passing Criteria: **70%**

No Negative Marking

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -h Weightage

1.	Forensic Science	15%
2.	Regulation, Policies and Ethics	10%
3.	Digital Evidence	20%
4.	Procedures and Methodologies	20%
5.	Digital Forensics	25%
6.	Tools/Systems/Programs	10%
	Total	100%

$: CHFI -h Modules

1.	Computer forensics in Today's world
2.	Computer Forensics Investigation Procedure
3.	Understanding Hard Disks and file Systems
4.	Data Acquisition and Duplication
5.	Defeating Anti-forensics techniques
6.	Operating System forensics
7.	Network Forensics

8.	Investigating Web Attacks
9.	Database Forensics
10.	Cloud Forensics
11.	Malware Forensics
12.	Investigating Email crimes
13.	Mobile Forensics
14.	Forensics Report Writing and Presentation

™

Computer Hacking Forensic INVESTIGATOR

$: CHFI -h PANIC

DO I WANT THIS?

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -h begin

Two approaches to study:

1. Self Study -> Official Content
2. Official content -> Self Study (Preferred)

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -begin

To register, you can start by visiting:

https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/

->Get Certified->Fill in the details and Wait

Self Assessment:

https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/assessment/

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -content

1 Year Access to:

- Subscription to Official Videos
- Subscription to Official Courseware
- Exam Voucher

6 Months Access to:

- iLabs

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -approach

Go through the content

- Gives you Insight of depth of knowledge required and scope
- Make notes of what you don't know or have little knowledge around

Go through iLabs

- Beginners: Gives you hands on experience on variety of tools, must do!
- Intermediate: Just screenshots and move on!

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -approach | more

While (Target date is not near) OR (Exhausted content):

- Download more content
- Append the new content to your notes
- Go through your notes
- Give Practice test
  - Note down questions which you made a guess to answer
  - Find out why an answer is right, and why other options are wrong
- Find out knowledge gaps
- Improvise Notes

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -approach | more

When target date is near:

- Cut short notes
- Remove clutter that you are 100% sure you will be able to answer
- Revise, Revise, Revise

$: CHFI -Examtime

Scheduling Exam:

Schedule on any suitable day (Mon – Fri)

Exam timings is based on EDT Time zone

- EDT 3:00 PM = 12:30 AM IST

Reschedule Exam 48 Hours of planned Exam Time

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -Examtime

Exam Process

- You should be alone
- No additional displays connected to your machine
- Follow the instructions

Exam Results;

- Immediate Results
- Phew!
- Retake: https://cert.eccouncil.org/exam-retake-policy.html
- Retake Cost: 350 USD

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -Finish

Digital certificate in 5 working days

Physical Certificate in 45 days

C|HFI™ Computer Hacking Forensic INVESTIGATOR

$: CHFI -Reference

S.No	Description	Link
1	CHFI Blue Print – EC Council	http://bit.ly/nullmeetchfi1
3	Official CHFI Candidate Handbook	http://bit.ly/nullmeetchfi3
4	Cybrary CHFI Course	http://bit.ly/nullmeetchfi4
5	Cybrary CHFI Self Study Guide	http://bit.ly/nullmeetchfi5
6	CHFI All-in-One Exam Guide	http://bit.ly/nullmeetchfi6
7	CHFI Crash Study Guide	http://bit.ly/nullmeetchfi7
8	Udemy CHFI Practice Test + Notes	http://bit.ly/nullmeetchfi8
9	Udemy CHFI Another Practice Test	http://bit.ly/nullmeetchfi9
10	CHFI Official Assessment Link	http://bit.ly/nullmeetchfi10

HFI™ Hacking Forensic INVESTIGATOR

>>> sys.exit()

Thanks!

Any questions