Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Ethical Hacking and Countermeasures Ethical Hacking Essential Concepts - II	Exam 312-50 Certified Ethical Hacker
SOC Workflow	CEH
COLLECT Log data are collected from various devices on the network and sent it to the SEM INGEST Threat Data Contextual Data Contextual Data VALIDATE SoC analysts look for indicators of compromise data are ingested into SIEM for event correlation and identification of anomalies VALIDATE Validate incidents Validate incidents Validate incidents Validate incidents Validate incidents	the incidents and incident for business audit incident sand business audit incident purposes and ough a response lessons learned
LO#12: Explain Different Phases of Computer Forensic Investigation	
Copyright © by SP-Costedil, All Rights Reserved, Reproduction is Strictly Production of	
Notes:	
Appendix B Page 3755 Ethical Ho	acking and Countermeasures Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Computer Forensics



 Computer Forensics refer to a set of methodological procedures and techniques that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, whereby any evidence discovered is acceptable during a legal or administrative proceeding

Objectives of Computer Forensics:

- To track and prosecute cyber crime perpetrators
- To gather evidence of cyber crimes in a forensically sound manner
- To estimate the potential impact of a malicious activity on the victim and assess the intent of the perpetrator
- To find vulnerabilities and security loopholes that help attackers
- To recover deleted files, hidden files, and temporary data that could be used as evidence

provide C by TC-Council, All Earlier Reserved, Reproduction is Strictly Probbited.

Phases Involved in the Computer Forensics Investigation Process



Pre-investigation Phase

- Deals with tasks to be performed prior to commencing the actual investigation
- Involves setting up a computer forensics lab, building a forensics workstation, developing an investigation toolkit, setting up an investigation team, gaining approval from the relevant authority, and so on

Investigation Phase

- 9 The main phase of the computer forensics investigation process
- Involves the acquisition, preservation, and analysis of evidentiary data to identify the source of the crime and the culprit behind it

Post-investigation Phase

- Deals with the documentation of all the actions undertaken and findings uncovered during an investigation
- Ensures that the report is well explicable to the target audience, and provides adequate and acceptable evidence

Copyright © by EC-Cossol I. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: _____

Appendix B Page 3756

Ethical Hacking and Countermeasures Copyright © by **EC-Council**All Rights Reserved. Reproduction is Strictly Prohibited.