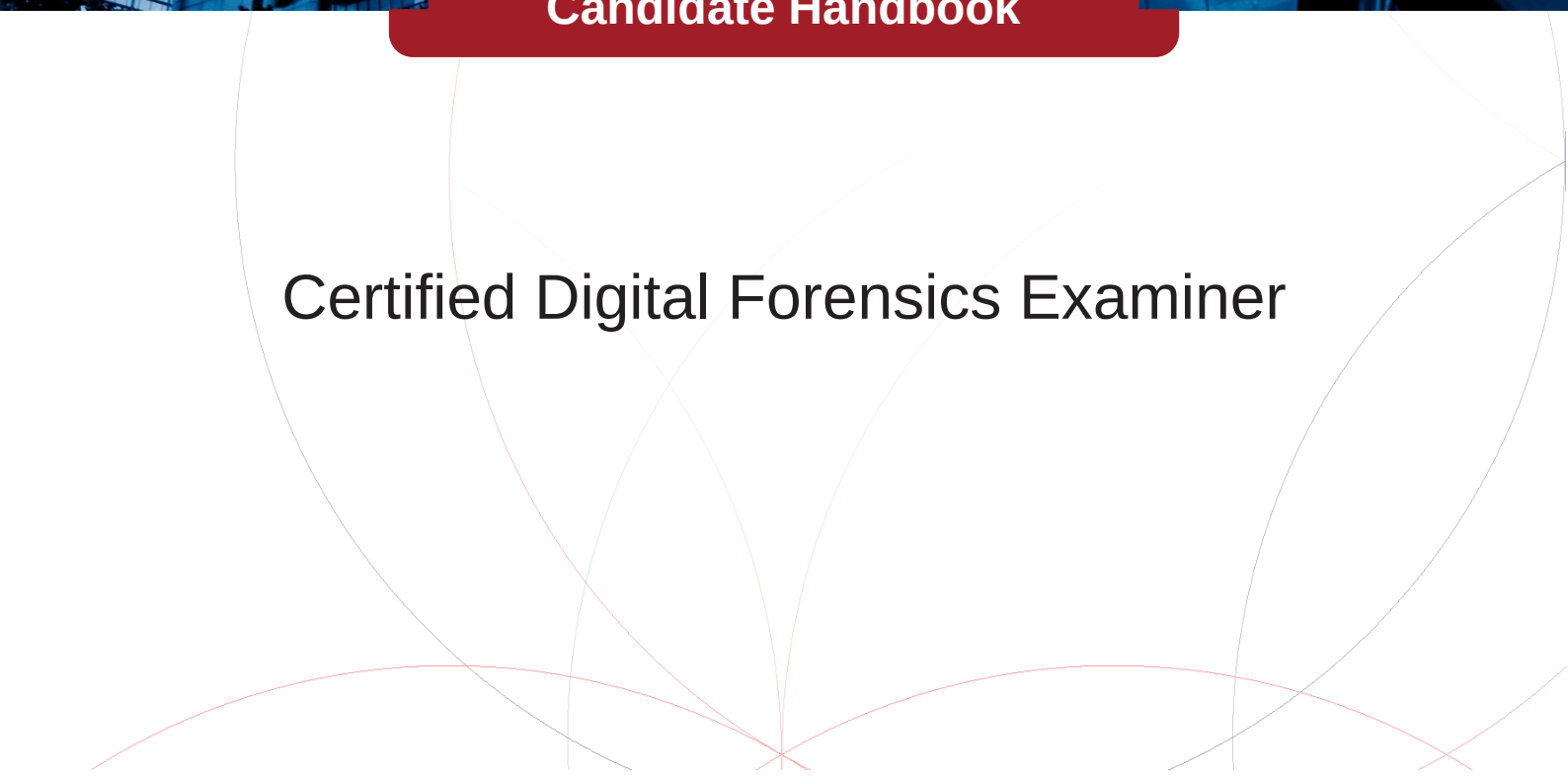




PECB

Candidate Handbook

Certified Digital Forensics Examiner



Contents

SECTION I: INTRODUCTION.....	3
About PECB.....	3
Accreditations and Affiliations	3
PECB Code of Ethics.....	3
Introduction to Certified Digital Forensics Examiner Certification.....	4
SECTION II: EXAM PROCESS, RULES AND POLICIES	5
Preparing For and Scheduling the Exam.....	5
Special Accommodations.....	5
Taking the Exam.....	5
Exam Results.....	6
Exam Retake Policy.....	6
Exam Security Policy	6
Exam Competency Domains	7
Sample Exam Questions.....	13
SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES	15
PECB Certified Digital Forensics Examiner Credentials.....	15
Applying for Certification	15
Professional Experience	16
Professional References	16
Project Experience	16
Evaluation of Certification Applications.....	16
SECTION IV: CERTIFICATION MAINTENANCE POLICY	17
Renewing the Certification	17
Upgrade Credentials.....	17
Suspension of Certification	17
Revocation of Certification.....	17
Other Statuses.....	17
SECTION V: OTHER POLICIES	18
Application Fees for Examination and Certification	18
Complaint and Appeal Policy	18
Exams from Other Accredited Certification Bodies.....	18
Refund Policy.....	18

SECTION I: INTRODUCTION

About PECB¹

PECB is a leading certification body dedicated to fostering digital trust through comprehensive education, certification, and certificate programs across various disciplines. We empower professionals to develop and demonstrate their competence in digital security and other areas of expertise by providing world-class certification programs that adhere to internationally recognized standards.

Vision: As the global leader in digital trust education and certification, our vision is to empower and inspire professionals by enhancing their skills and fostering their professional success.

Mission: Our mission is to empower professionals with the knowledge and skills to protect their digital assets and ensure business continuity. Through our comprehensive programs, we aim to foster a secure digital ecosystem where innovation thrives and risks are managed effectively.

Values: Growth, Change, Harmony, Simplicity, Reliability, and Quality

Accreditations and Affiliations

At PECB, we are driven and culturally powered by a systemic process of continual improvement and professional development. As a testament to our high standards and commitment to providing quality services to our clients, PECB is accredited by a number of bodies and is a member of many professional organizations.

For detailed information on our accreditations and affiliations, click [here](#).

PECB Code of Ethics

The Code of Ethics is the set of values that PECB is committed to following, and defines the responsibilities of PECB professionals, including employees, trainers, examiners, invigilators, members of different committees, partners, distributors, certified individuals, and certificate holders. To read the PECB's Code of Ethics, click [here](#).

¹ Notes:

- The legal name of PECB is "PECB Group Pte. Ltd."
- PECB is an acronym that stands for "Professional Evaluation and Certification Board."
- Education (used in the first sentence of this page) refers to training courses developed by PECB, and offered globally through its network of partners.
- Certification refers to certification services provided according to ISO/IEC 17024. Certificate Program refers to certificate program services provided according to ANSI/ASTM E2659.
- "Certified" refers to ISO/IEC 17024 certifications' requirements and "Certificate holder" refers to ASTM E2659 certificate programs' requirements. Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

Introduction to Certified Digital Forensics Examiner Certification

This document specifies the PECB Certified Digital Forensics certification scheme in compliance with ISO/IEC 17024. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your certification application.

If you have questions or need further information after reading it, please contact support@pecb.com.

SECTION II: EXAM PROCESS, RULES AND POLICIES

For detailed and most up-to-date information, you are advised to refer to the online **Exam Rules and Policies** by clicking [here](#).

Preparing For and Scheduling the Exam

To schedule the exam, candidates have two options:

1. **Online:** Through the [PECB Exams application](#). To schedule a remote exam, please go to the following link: [Exam Events](#).
2. **Paper-based:** By contacting the PECB authorized partner that provided the training course. The partner arranges the date, time, and location where the candidate is going to attend the exam.

For any changes with regard to the exam date, time, location, or other details, please contact support@pecb.com.

Special Accommodations

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of special needs (dyslexia, dyspraxia, ADHD, vision impairment, but not limited to) and temporary conditions (pregnancy, surgery, postoperative recovery, but not limited to), they can apply for such arrangements through the [myPECB](#) dashboard/ Enroll for an Exam. Any information that candidates provide regarding their special needs will be treated with confidentiality.

Taking the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not receive additional time to make up for the delay and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (national ID card, driver's license, or passport) and show it to the invigilator.

Online Exam Rules	Paper-Based Exam Rules
• Exams are provided electronically via the PECB Exams application. • The use of secondary electronic devices, such as tablets and phones, is not allowed during the exam. • The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera. • If requested on the day of the exam, additional time can be provided to candidates taking the exam in a non-native language, as follows: – 10 additional minutes for Foundation exams – 20 additional minutes for Manager exams – 30 additional minutes for Lead exams	• Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. • The use of electronic devices, such as laptops, tablets, or phones, is not allowed. • The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course. • If requested on the day of the exam, additional time can be provided to candidates taking the exam in a non-native language, as follows: – 10 additional minutes for Foundation exams – 20 additional minutes for Manager exams – 30 additional minutes for Lead exams

For specific information on exam types, languages available, and other details, please check the [List of PECB Exams](#).

Exam Results

Exam results will be communicated via email.

- The time span for the communication of exam results starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

If candidates disagree with the evaluation, they may request a re-evaluation of their exam results within 30 days from the date they receive their exam results. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes. For more information, please visit this link: [Exam Rules and Policies - PECB](#).

Exam Security Policy

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams.

Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals who violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking/invalidating any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam Competency Domains

The content of the exam is divided as follows:

Domain 1: Network traffic and protocol analysis

Main objective: Ensure that the candidate is able to understand, analyze, and interpret network traffic, protocols, and communication patterns to identify normal behavior, detect anomalies, and support security monitoring and incident investigation activities.

Competencies	Knowledge statements
1. Ability to explain the role of network and traffic analysis in digital forensics investigations	1. Knowledge of the principles of network communications and their relevance to digital forensic investigations.
2. Ability to identify and analyze network traffic relevant to forensic evidence collection	2. Knowledge of methods for capturing, preserving, and analyzing network traffic as forensic evidence.
3. Ability to use Wireshark display filters and capture filters to isolate network traffic	3. Knowledge of tools and techniques used for network traffic forensic analysis (e.g., packet capture and flow analysis).
4. Ability to interpret network protocols and communications from a forensic perspective	4. Understand how Wireshark captures packets and applies display/capture filters
5. Ability to analyze network activity using structured log data (e.g., Zeek logs)	5. Knowledge of network protocols and how they are interpreted in traffic analysis
6. Ability to reconstruct network events and timelines using captured traffic and logs	6. Knowledge of Zeek architecture (event engine and scripting engine) and common Zeek logs (conn.log, dns.log, http.log, ssl.log) for network analysis
7. Ability to identify suspicious or malicious network activity during forensics analysis	7. Understand how network traffic evidence supports event reconstruction, attribution, and root cause analysis.
8. Ability to preserve network traffic evidence while maintaining integrity and chain of custody	8. Knowledge of normal vs abnormal network behavior and how it indicates malicious activity
9. Ability to correlate network traffic data with other digital forensic artifacts	9. Knowledge of legal, procedural, and evidentiary requirements related to network traffic in digital forensics.
	10. Understand techniques for correlating network traffic data with other digital forensic artifacts
	11. Knowledge of legal, procedural, and evidentiary requirements related to network traffic in digital forensics

Domain 2: Memory acquisition and forensics

Main objective: Ensure that the candidate is able to understand, perform, and document memory acquisition and memory forensic analysis activities in accordance with digital forensic principles, ensuring the integrity, reliability, and admissibility of volatile memory evidence.

Competencies	Knowledge statements
1. Ability to explain the purpose and importance of memory acquisition in digital forensic investigations	1. Knowledge of the principles of volatile memory, including RAM structure and behavior
2. Ability to identify different types of volatile memory and the data they contain	2. Knowledge of different types of volatile memory and the kinds of data they contain
3. Ability to perform memory acquisition using appropriate forensic methods and tools	3. Knowledge of memory acquisition techniques, tools (e.g., DumpIt, FTK Imager) and the importance of timely captures
4. Ability to preserve the integrity of memory evidence and maintain chain of custody	4. Understand forensic requirements for evidence integrity, chain of custody, and repeatability during memory acquisition
5. Ability to analyze memory dumps to identify relevant forensic artifacts	5. Knowledge of common memory artifacts such as running processes, loaded modules, network connections, and credentials
6. Ability to recognize indicators of malicious activity within volatile memory	6. Understand common malware and attack techniques that leave artifacts in memory
7. Ability to correlate memory forensic findings with other digital evidence sources	7. Be familiar with the techniques for correlating memory forensic findings with other digital evidence sources
8. Ability to document and report memory acquisition and analysis results in a forensically sound manner	8. Knowledge of forensic documentation and reporting requirements for memory analysis

Domain 3: File-system and disk forensics

Main objective: Ensure that the candidate is able to perform disk and file-system forensic activities, including acquisition, analysis, and interpretation of storage media, in a forensically sound manner while preserving evidence integrity and supporting investigative and legal requirements.

Competencies	Knowledge statements
1. Ability to explain the principles and objectives of disk and file-system forensics	1. Knowledge of the principles and objectives of disk and file-system forensics in investigations
2. Ability to perform forensic acquisition of storage media using appropriate methods and tools	2. Knowledge of disk acquisition techniques, including logical and physical imaging methods
3. Ability to preserve disk evidence integrity and maintain proper chain of custody	3. Understand forensic requirements for evidence integrity, validation, and repeatability
4. Ability to analyze file systems to identify relevant forensic artifacts	4. Knowledge of the structure and functioning of common file systems (e.g., NTFS, FAT, exFAT, ext) and artifacts such as metadata, timestamps, slack space, and unallocated space
5. Ability to recover deleted, hidden, or fragmented files from storage media	5. Understand techniques for file recovery, carving, and analysis of deleted data
6. Ability to interpret file metadata and timelines during forensic investigations	6. Be familiar with metadata and timeline analysis techniques and tools for reconstructing events used for timeline analysis and reconstruction
7. Ability to correlate disk forensics findings with other digital evidence sources	7. Knowledge of techniques for correlating disk forensic findings with other digital evidence sources
8. Ability to document and report disk and file-system forensic findings in a clear and legally defensible manner	8. Knowledge of legal, procedural, and evidentiary considerations related to disk evidence in digital forensics

Domain 4: Malware analysis and reverse engineering

Main objective: Ensure that the candidate is able to analyze, classify, and investigate malicious software using forensic and reverse-engineering techniques to understand malware behavior, identify indicators, and support digital forensic investigations and incident reconstruction.

Competencies	Knowledge statements
1. Ability to explain the objectives and scope of malware analysis within digital forensics	1. Knowledge of the objectives and scope of malware analysis in digital forensics
2. Ability to identify different types of malware and their characteristics	2. Knowledge of common malware types, such as viruses, worms, trojans, ransomware, spyware, and rootkits
3. Ability to perform basic static malware analysis to extract relevant information	3. Knowledge of static malware analysis techniques such as file inspection, hashing, and string analysis
4. Ability to perform basic dynamic malware analysis in a controlled environment	4. Knowledge of dynamic malware analysis techniques such as behavioral analysis and sandboxing
5. Ability to apply reverse-engineering techniques to analyze malicious code behavior	5. Be familiar with basic reverse-engineering concepts (e.g., code disassembly, debugging)
6. Ability to identify indicators of compromise derived from malware analysis	6. Knowledge of tools used in malware analysis and reverse engineering (e.g., Ghidra, IDA Pro, Volatility, sandbox environments)
7. Ability to correlate malware analysis findings with other forensic evidence sources	7. Knowledge of common malware analysis behaviors (e.g., command-and-control communication, data exfiltration, and privilege escalation), infection vendors, and persistence mechanisms
8. Ability to create and apply YARA rules for malware detection and classification	8. Knowledge of techniques for correlating malware analysis findings with other forensic evidence sources
9. Ability to document and report malware analysis results in a clear and forensically sound manner	9. Understand YARA rule structure (strings, conditions, metadata) and how it is used for malware detection and hunting
	10. Knowledge of legal, ethical, and safety considerations when handling and analyzing malicious software

Domain 5: Threat hunting, automation, and correlation

Main objective: Ensure that the candidate is able to proactively identify, analyze, and correlate threats and malicious activities using threat-hunting techniques, automation, and data correlation to support digital forensic investigations and incident reconstruction.

Competencies	Knowledge statements
1. Ability to explain the role of threat hunting in digital forensic investigations	1. Understand the principles and objectives of threat-hunting within digital forensics
2. Ability to formulate threat-hunting hypotheses based on forensic evidence and intelligence	2. Knowledge of common threat-hunting methodologies, analytical approaches, and attacker TTPs
3. Ability to analyze large volumes of data to identify suspicious or malicious patterns	3. Knowledge of data sources (e.g., logs, memory artifacts, disk artifacts, and network artifacts) and analytical techniques for identifying patterns in large datasets
4. Ability to correlate data from multiple sources to reconstruct attacker activities	4. Knowledge of techniques for correlating events and artifacts across multiple evidence sources
5. Ability to identify indicators of compromise and attacker behaviors through correlation	5. Understanding indicators of compromise and how they are identified through data correlation
6. Ability to apply automation techniques to support forensic analysis and threat detection	6. Understand automation concepts and how scripting or tools support forensic investigations
7. Ability to create and apply YARA rules for threat detection and hunting	7. Understand YARA rule structure and use in identifying malware patterns
8. Ability to validate and document threat-hunting findings in a forensically sound manner	8. Knowledge of documentation, validation, and legal considerations related to threat-hunting findings in digital forensics
9. Ability to integrate threat-hunting results into broader digital forensic investigations and reporting	9. Understand how threat hunting supports incident reconstruction, attribution, and root cause analysis

Based on the above-mentioned domains and their relevance, the exam contains 20 hands-on practice questions, as summarized in the table below:

		Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	Level of understanding (Cognitive/Taxonomy) required	
				Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Network traffic and protocol analysis	4	20	X	
	Memory acquisition and forensics	4	20		X
	File-system and disk forensics	4	20		X
	Malware analysis and reverse engineering	4	20	X	
	Threat hunting, automation, and correlation	4	20		X
Total		20	100%		
Number of questions per level of understanding				12	8
% of the exam devoted to each level of understanding (cognitive/taxonomy)				60%	40%

The passing score of the exam is **70%**.

This exam comprises hands-on practical questions: The hands-on lab exam is designed to evaluate candidates' ability to apply their knowledge and skills in practical, real-world contexts. Candidates are expected to demonstrate technical proficiency by configuring, troubleshooting, and optimizing systems; analyzing and solving problems; and integrating multiple concepts to achieve functional solutions. The exam emphasizes practical competence, accuracy, and efficiency, focusing on how well candidates can translate theoretical understanding into effective technical execution.

This is an open-book exam. The candidate is allowed to use the following reference materials:

- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)
- A hard copy dictionary

A sample of exam questions will be provided below.

Sample Exam Questions

1. What is the main purpose of the .text section header highlighted in the screenshot?

To store executable program instructions

```
student@desktop:~/Desktop$ readelf --sections /home/student/Desktop/hello
There are 29 section headers, starting at offset 0x1930:

Section Headers:
 [Nr] Name              Type              Address            Offset
      Size              EntSize          Flags    Link  Info  Align
 [ 0]                      NULL              0000000000000000  00000000
      0000000000000000  0000000000000000  0      0      0
 [ 1] .interp              PROGBITS          0000000000000238  00000238
      000000000000001c  0000000000000000  A      0      0      1
[14] .text                PROGBITS          0000000000000540  00000540
      00000000000001a2  0000000000000000  AX      0      0      16
```

2. Based on the VirusTotal detection report shown in the screenshot, how is the analyzed file categorized?

Trojan/spyware

62 / 73
Community Score -51

62/73 security vendors flagged this file as malicious

8b2e701e91101955c73865589a4c72999aeabc11043f712e05fdb1c17c4ab19a

Size: 249.00 KB

Last Analysis Date: 1 month ago

ShellExtension

peexe spreader detect-debug-environment direct-cpu-clock-access idle checks-user-input runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 23+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.zbot/foreign

Threat categories: trojan spyware

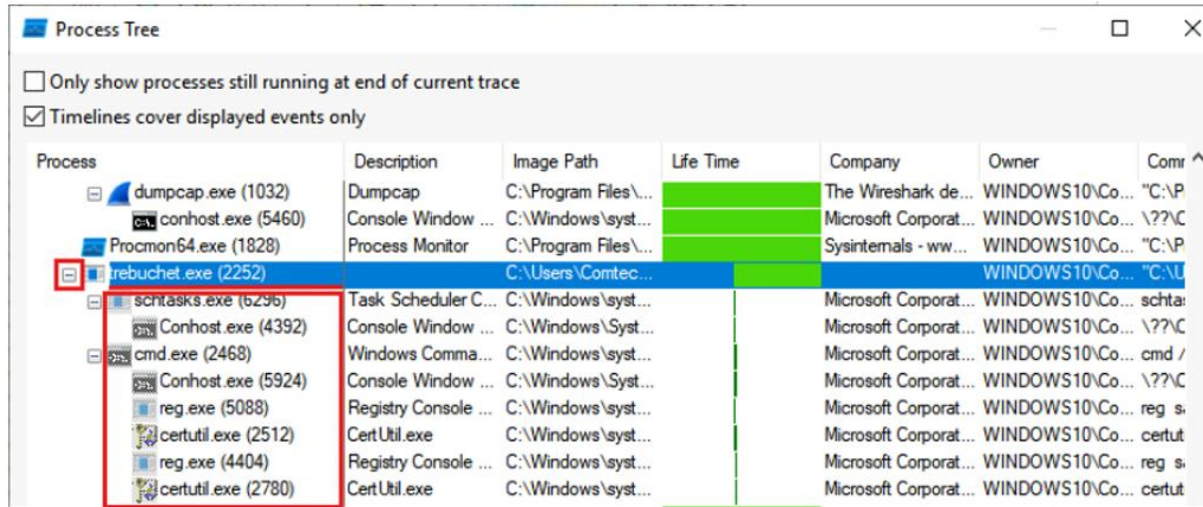
Family labels: zbot foreign ikzv

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Acronis (Static ML)	Suspicious	Alibaba	TrojanSpy:Win32/Obfuscator.c21d32b2
AliCloud	Trojan(spy):Win/Zbot.AMV	ALYac	Trojan.Foreign.Gen.2
Antiy-AVL	Trojan(Spy)/Win32.Zbot	Arcabit	Trojan.Foreign.Gen.2
Arctic Wolf	Unsafe	Avast	Win32:Cryptor
AVG	Win32:Cryptor	Avira (no cloud)	TR/Spy.Zbot.ikzv
BitDefender	Trojan.Foreign.Gen.2	Bkav Pro	W32.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.generic
Cynet	Malicious (score: 99)	Deepinstinct	MALICIOUS
DrWeb	Trojan.PWS.Panda.655	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Foreign.Gen.2 (B)	eScan	Trojan.Foreign.Gen.2
ESET-NOD32	Win32/Spy.Zbot.AAQ	Fortinet	W32/Kryptik.CLOOitr
GData	Trojan.Foreign.Gen.2	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Downloader.oais1	Huorong	Trojan/GenericIE36B1C507C300350

3. Based on the Process Tree shown in the screenshot, which process was executed first by the trebuchet.exe malware?

schtasks.exe



Process	Description	Image Path	Life Time	Company	Owner	Comr ^
dumpcap.exe (1032)	Dumpcap	C:\Program Files\...		The Wireshark de...	WINDOWS10\Co...	"C:\P
conhost.exe (5460)	Console Window ...	C:\Windows\syst...		Microsoft Corporat...	WINDOWS10\Co...	\??\C
Procmon64.exe (1828)	Process Monitor	C:\Program Files\...		Sysinternals - ww...	WINDOWS10\Co...	"C:\P
trebuchet.exe (2252)		C:\Users\Comtec...			WINDOWS10\Co...	"C:\U
schtasks.exe (6296)	Task Scheduler C...	C:\Windows\syst...		Microsoft Corporat...	WINDOWS10\Co...	schtas
Conhost.exe (4392)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	WINDOWS10\Co...	\??\C
cmd.exe (2468)	Windows Comma...	C:\Windows\syst...		Microsoft Corporat...	WINDOWS10\Co...	cmd /
Conhost.exe (5924)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	WINDOWS10\Co...	\??\C
reg.exe (5088)	Registry Console ...	C:\Windows\syst...		Microsoft Corporat...	WINDOWS10\Co...	reg s
certutil.exe (2512)	CertUtil.exe	C:\Windows\syst...		Microsoft Corporat...	WINDOWS10\Co...	certut
reg.exe (4404)	Registry Console ...	C:\Windows\syst...		Microsoft Corporat...	WINDOWS10\Co...	reg s
certutil.exe (2780)	CertUtil.exe	C:\Windows\syst...		Microsoft Corporat...	WINDOWS10\Co...	certut

SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES

PECB Certified Digital Forensics Examiner Credentials

All PECB certifications have specific requirements regarding professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB Certified Digital Forensics Examiner scheme have the following requirements:

Credential	Exam	Professional experience	Computer forensics project experience	Other requirements
PECB Certified Provisional Digital Forensics Examiner	PECB Certified Digital Forensics Examiner exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Digital Forensics Examiner (CDFE)	PECB Certified Digital Forensics Examiner exam or equivalent	Five years: two years of work experience in computer forensics	300 hours	Signing the PECB Code of Ethics

To be considered valid, the implementation activities should follow best implementation and management practices and include the following:

1. Performing comprehensive forensic examination of computers, mobile devices, storage media, and cloud infrastructure
2. Preserving data integrity and chain of custody throughout evidence collection and handling
3. Analyzing file systems, network logs, and memory captures to reconstruct user and system activity
4. Collaborating with law enforcement, legal counsel, and corporate security teams on evidence requirements and case strategy
5. Developing and enforcing digital-forensics best practices, policies, and standard operating procedures
6. Leading incident response efforts focused on digital evidence acquisition, analysis, and remediation

For detailed and most up-to-date information, you are advised to refer to the online **Certification Process** by clicking [here](#).

Applying for Certification

All participants who successfully pass their certification exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific professional requirements will need to be fulfilled to be PECB certified.

The application process is very simple and takes only a few minutes:

- [Create](#) your account
- Check your email for the confirmation link
- [Log in](#) and click on Apply for Certificate

The approval of the application occurs when the Certification Department validates that you fulfil all the certification requirements regarding the credential you have applied for. An email will be sent to the address you provided during your application to update you on your application status. If approved, you will then be able to download your certificate and digital badge from your member account.

Professional Experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the CV.

Professional References

For each application, two professional references are required. Professional references shall be individuals who have worked with you in a professional environment and can validate your expertise in the respective field, current, and previous work history. You cannot use as a reference the persons who fall under your supervision or are a relative of yours.

Project Experience

The candidate's project log will be checked to ensure that the candidate has the required number of implementation hours.

Evaluation of Certification Applications

The Certification Department will evaluate each application to validate the candidates' eligibility for certification or certificate program. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates' credential downgrade.

PECB can deny certification/certificate program if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics
- Fail the exam

If applicants have any concerns regarding the denial of certification/certificate program, they may file an appeal by following the complaint and appeal process [Complaint and Appeal Policy](#).

The application payment for the certification/certificate program is nonrefundable. This is due to the application verification process, the evidence submitted by the candidates, and the involvement of the relevant departments.

If candidates pass the exam, they can apply for the certificate within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing to certification.team@pecb.com and pay the required fee.

SECTION IV: CERTIFICATION MAINTENANCE POLICY

For detailed and most up-to-date information, you are advised to refer to the online **Certification Maintenance Policy** by clicking [here](#).

Renewing the Certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continuing professional development (CPD) hours. In addition, they need to pay the annual maintenance fee.

Upgrade Credentials

PECB Certifications can be upgraded online through your dashboard by logging in [here](#), clicking **View Certificate**, and then clicking the **Upgrade** button. For more information on the upgrade requirements and fees, go to the [Certification Maintenance](#) page on the PECB website.

Suspension of Certification

Failure to submit the CPD and AMF payment during the certification cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs. In addition to these, the certification may be suspended for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been suspended are not authorized to further promote their certification while it is suspended.

Suspended members must remediate their suspension within a maximum period of 12 months.

Revocation of Certification

PECB can revoke (that is, withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. In addition to these, certification may be revoked for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been revoked are not authorized to use any references to a certified status.

<https://pecb.com/en/about/complaint-and-appeal-policy>

If candidates disagree with any certification decision (certification level, suspension, or revocation) they may request a re-evaluation within 30 days from the date they receive their certification decision. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus. For more information, go to the [Certification Maintenance](#) page on the PECB website.

SECTION V: OTHER POLICIES

Application Fees for Examination and Certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: \$1000²
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is as follows:

- Master Certification: \$100
- Foundation Certification: \$200
- Transition Certification: \$200
- All other Certifications: \$500

For candidates who complete a training, eLearning, or self-study course delivered by a PECB Partner, the training fee includes the first exam attempt, one free retake, the certification application fee, and the first year of the Annual Maintenance Fee (AMF). This cycle must be completed within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats.

Complaint and Appeal Policy

A person wishing to file a complaint or an appeal can do so by submitting a [service ticket](#) and selecting the corresponding category in the topic dropdown menu: “file a complaint” or “file a certification/certificate program appeal”. Before filing a complaint or an appeal, make sure to follow the [complaint and appeal policy](#).

Exams from Other Accredited Certification Bodies

PECB accepts exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective exam(s) can be accepted as equivalent to the respective PECB certification.

Refund Policy

PECB will refund your payment if the requirements of the Refund Policy are met. To read the Refund Policy, click [here](#).

² All prices listed in this document are in US dollars.



Contact PECB Support at
support@pecb.com



Telephone number
+1-844-426-7322



Visit our [Help Center](#) to access manuals, FAQs, and quick guides, or reach us directly via Live Chat or by submitting a ticket [here](#).

Follow us on:



www.pecb.com