

中央警察大學 105 學年度碩士班入學考試試題

所 別：資訊管理研究所

科 目：電腦犯罪與資訊安全

作答注意事項：

1. 本試題共 4 題，每題各占 25 分；共 2 頁。
2. 不用抄題，可不按題目次序作答，但應書寫題號。
3. 禁用鉛筆作答，違者不予計分。

一、The Scientific Working Group on Digital Evidence (SWGDE) creates standards for digital and multimedia evidence. In the document of **SWGDE Best Practices for Computer Forensics** Version 3.1 (September 05, 2014), it describes the following concepts of ‘Evidence Triage/Preview.’

- (一) Evidence triage may not be appropriate for all situations.
- (二) Evidence preview may miss items of evidentiary value.
- (三) Time and date stamps may be affected by the evidence triage/preview process on live systems.
- (四) An evidence preview/triage shall not take the place of a complete exam.

Please explain the above issues in details.

二、Security assessments can be one of two types: a security audit (vulnerability assessment) or a penetration test. The security audit scans and tests a system or network for existing vulnerabilities but does not intentionally exploit any of them. A penetration test actively seeks to exploit vulnerabilities encountered on target systems or networks. This shows the potential consequences of a hacker breaking in through unpatched vulnerabilities.

Please translate the above paragraph into Chinese (15 分), and list the pen test methodology. (10 分)

三、解釋名詞：

- (一) Deception Defense System
- (二) ICMP flooding
- (三) Pretty Good Privacy
- (四) Secure Electronic Commerce
- (五) Kerberos Authentication

四、請回答下列問題：

- (一) 網路防火牆依功能可分為以下 3 種：(1) Packet Filter、(2) Application Level Gateway、(3) Circuit Level Gateway。請分別說明之。(15 分)
- (二) 當手機被植入竊聽軟體時，請說明如何查知與防制手機遭竊聽的方法。(10 分)