Câu hỏi trắc nghiệm

Phần 1: Kiến thức cơ bản về cấu trúc ZIP

1. **Tệp ZIP có thể được chia thành những phần chính nào?**

   A. Local File Header, Data Stream, File Trailer

   B. Local File Header, Central Directory Header, End of Central Directory

   C. File Header, File Descriptor, File Footer

   D. Local File Header, File Metadata, Archive Header

   Đáp án: B

2. **Định danh chữ ký (signature) của tệp ZIP là gì?**

   A. 0xCAFEBABE

   B. 0xDEADBEEF

   C. 0x504B0304

   D. 0x12345678

   Đáp án: C

3. **Trường thông tin bổ sung (Extra Fields) trong header của tệp ZIP được sử dụng để làm gì?**

   A. Mã hóa dữ liệu trong tệp ZIP

   B. Lưu thông tin mở rộng như dấu thời gian hoặc định danh người dùng

   C. Lưu trữ nội dung chính của tệp ZIP

   D. Chứa thông tin checksum CRC32

   Đáp án: B

Phần 2: Dấu vân tay tệp ZIP (File Fingerprints)

4. **Tại sao dấu vân tay tệp ZIP có thể khác nhau?**

A. Do cấu hình phần cứng của máy tính

B. Do ứng dụng và hệ điều hành tạo ra tệp

C. Do tệp nén có kích thước lớn hay nhỏ

D. Do cách sử dụng mã hóa trong tệp ZIP

Đáp án: B

5. **Dấu vân tay tệp ZIP có thể tiết lộ thông tin gì?**

A. Nội dung của tệp ZIP

B. Nguồn gốc của tệp, hệ điều hành, và ứng dụng sử dụng

C. Thời gian tải xuống từ Internet

D. Địa chỉ IP của máy tạo tệp

Đáp án: B

6. **Hệ điều hành nào sử dụng chuẩn thời gian FILETIME 64-bit trong tệp ZIP?**

A. Windows

B. macOS

C. Ubuntu

D. Android

Đáp án: A

Phần 3: Phân tích pháp y

7. **Khi phân tích tệp ZIP, "double zipping" là gì?**

A. Nén lại tệp ZIP đã được nén trước đó

B. Sử dụng hai phần mềm nén khác nhau để tạo tệp

C. Lưu trữ tệp ZIP trong hai thư mục khác nhau

D. Nén tệp ZIP mà không thay đổi cấu trúc ban đầu

Đáp án: A

8. **Một trong những công cụ nào sau đây không tạo thư mục __MACOSX khi nén tệp ZIP trên macOS?**

   A. Compress

   B. zip

   C. Bandizip

   D. WinZip

   Đáp án: B

9. **Trường nào trong tệp ZIP có thể chứa thông tin về múi giờ của hệ thống tạo tệp?**

   A. Local File Header

   B. Central Directory Header

   C. Extra Fields

   D. Data Descriptor

   Đáp án: C

Phần 4: Ứng dụng thực tế

10. **Nếu một tệp ZIP chứa nhiều dấu vân tay của các hệ thống khác nhau, điều này cho thấy gì?**

    A. Tệp ZIP bị hỏng

    B. Tệp ZIP được chỉnh sửa qua nhiều môi trường khác nhau

    C. Tệp ZIP không có giá trị pháp y

    D. Tệp ZIP có mã hóa đặc biệt

    Đáp án: B

11. Để phân loại tự động dấu vân tay tệp ZIP, hệ thống kiểm tra thông tin nào đầu tiên?

A. Dữ liệu CRC32

B. Sự tồn tại của các trường bổ sung trong header

C. Nội dung của tệp nén

D. Dung lượng tệp ZIP

Đáp án: B

Phần 5: Tổng hợp và mở rộng

12. Tệp ZIP trên hệ điều hành nào thường sử dụng mã hóa tên tệp CP949?

A. Windows với gói ngôn ngữ tiếng Hàn

B. macOS

C. Ubuntu

D. Windows với gói ngôn ngữ tiếng Anh

Đáp án: A

13. Thông tin UID và GID trong trường bổ sung của tệp ZIP có thể xác định gì?

A. Dung lượng tệp ZIP

B. Định danh người dùng và nhóm tạo tệp

C. Thời gian sửa đổi cuối cùng của tệp ZIP

D. Kiểu nén được sử dụng

Đáp án: B

14. Định dạng OOXML, như tài liệu MS Office, có thể được sử dụng để phân tích dấu vân tay không?

A. Có, vì nó sử dụng cấu trúc ZIP làm nền tảng

B. Không, vì nó không liên quan đến tệp ZIP

C. Chỉ với tài liệu PDF

D. Chỉ khi sử dụng hệ điều hành Linux

Đáp án: A

15. **Đâu là một ứng dụng tiềm năng của kỹ thuật phân tích dấu vân tay tệp ZIP?**

A. Xác định phần mềm nén sử dụng trong tội phạm mạng

B. Khôi phục dữ liệu bị mất từ tệp ZIP

C. Tăng tốc độ giải nén tệp ZIP lớn

D. Phát hiện mã độc trong tệp ZIP

Đáp án: A

Phần 6: Hệ điều hành và ứng dụng

16. **Những hệ điều hành nào đã được phân tích trong nghiên cứu này?**

A. Windows, macOS, và Android

B. Windows, macOS, và Ubuntu

C. macOS, Ubuntu, và iOS

D. Windows, Android, và iOS

Đáp án: B

17. **Một số ứng dụng có thể tạo ra các định dạng tệp OOXML là gì?**

A. Microsoft Office và LibreOffice

B. WinRAR và WinZip

C. 7-zip và Bandizip

D. Compress và zip

Đáp án: A

Phần 7: Mục tiêu và lợi ích

18. Mục tiêu của nghiên cứu về đặc điểm tệp ZIP là gì?

A. Xác định cấu trúc nén tốt nhất cho tệp ZIP

B. Phát triển phương pháp nén hiệu quả hơn

C. Xác định nguồn gốc tệp và theo dõi hành vi người dùng

D. Tăng tốc độ nén và giải nén tệp ZIP

Đáp án: C

19. Tại sao các đặc điểm của tệp ZIP được gọi là "dấu vân tay"?

A. Vì chúng đại diện cho hình ảnh thực của tệp ZIP

B. Vì chúng là duy nhất, phản ánh hệ điều hành và ứng dụng tạo tệp

C. Vì chúng giúp giải mã tệp ZIP nhanh hơn

D. Vì chúng liên quan đến cấu trúc mã hóa tệp

Đáp án: B

20. Lợi ích chính của phân tích đặc điểm tệp ZIP trong điều tra pháp lý kỹ thuật số là gì?

A. Xác định kích thước tối ưu cho tệp ZIP

B. Giảm thời gian giải nén tệp ZIP trong điều tra

C. Xác định nguồn gốc và môi trường tạo tệp để hỗ trợ điều tra

D. Phát hiện virus trong tệp ZIP

Đáp án: C