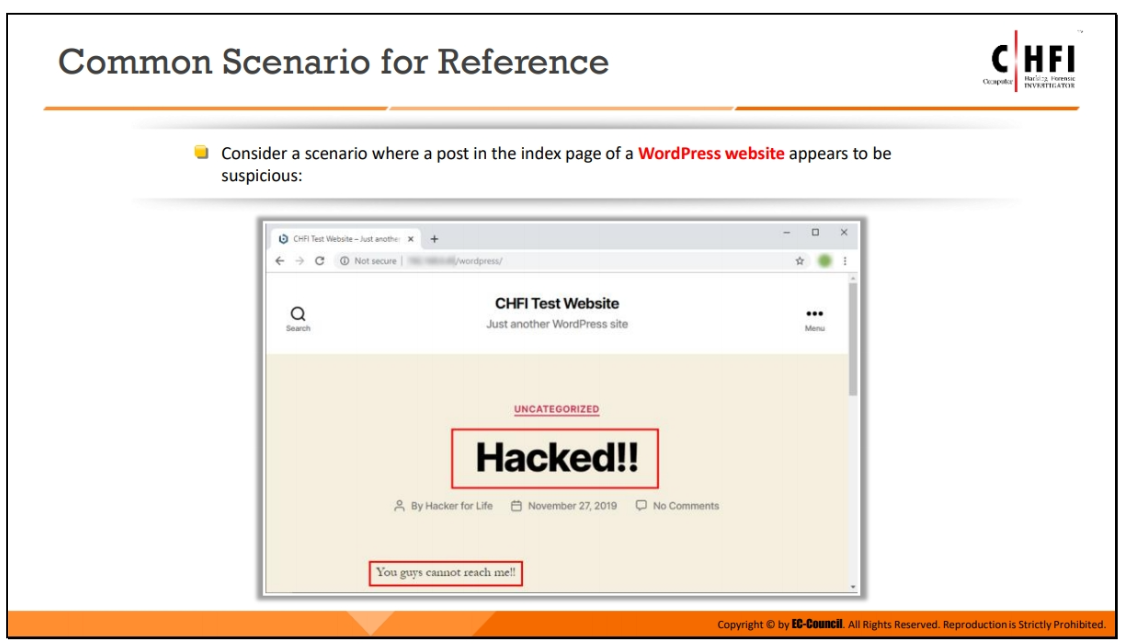
# LO#07: Thực hiện điều tra số trên cơ sở dữ liệu ứng dụng Web WordPress

Để thuận tiện cho quá trình điều tra số trên máy chủ MySQL, chúng tôi thực hiện một kịch bản mà trong đó một trang web WordPress được cho là đang bị xâm phạm. Phần này ta tập chung vào điều tra bằng cách chia nó thành 2 kịch bản :

1. Kịch bản đầu tiên là làm thế nào để xác định người dùng độc hại và các bài đăng của họ trong cơ sở dữ liệu WordPress. Cuộc điều tra này đã được tiến hành bằng các dòng lệnh.
2. Kịch bản thứ hai là trình bày cách kiểm tra các tệp nhị phân có trên máy chủ MySQL và lấy thêm thông tin liên quan đến các giao dịch xảy ra trong cở sở dữ liệu và khôi phục dữ liệu bị xóa bởi những người dùng độc hại.



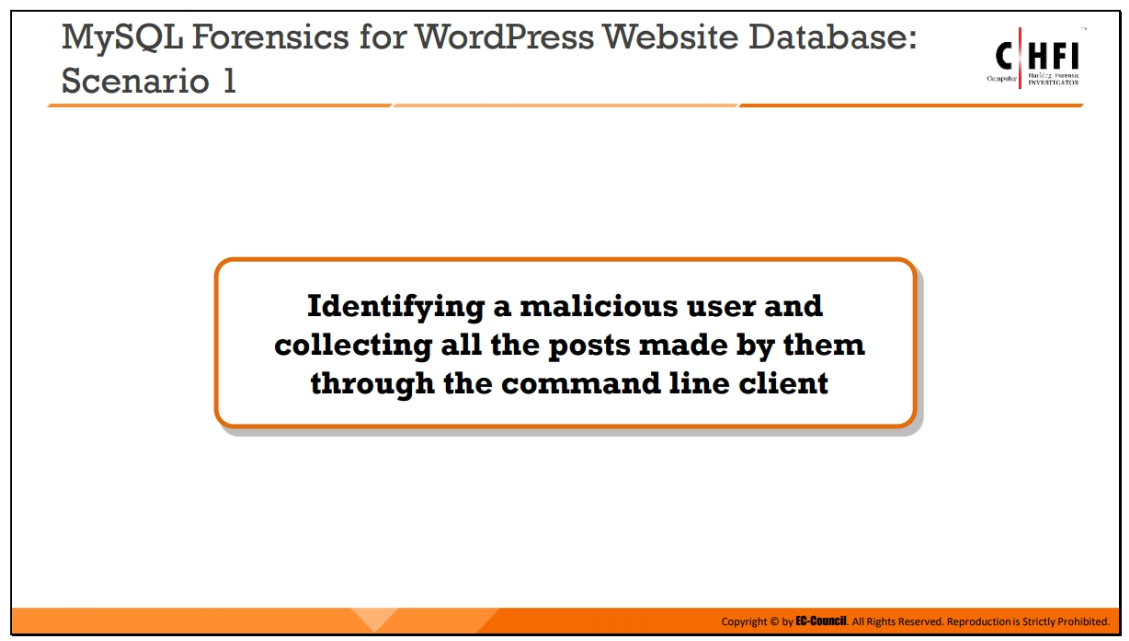
**Kịch bản chung để tham khảo**

Các quản trị viên thường là những người chịu trách nhiệm quản lý các trang web WordPress sử dụng các hệ quản trị cơ sở dữ liệu MySQL và phpMyAdmin. Đôi khi, họ có thể không tuân theo các phương pháp hay nhất về bảo mật, chẳng hạn như cập nhật WordPress

plugin và triển khai mật khẩu mạnh để đăng nhập MySQL; điều này dẫn đến việc để lại các backdoor có thể được sử dụng bởi những kẻ tấn công để giành quyền truy cập vào ứng dụng web hoặc đôi khi là chính hệ quản trị cơ sở dữ liệu.

Ở đây, chúng tôi xem xét một trang web WordPress có chứa một bài đăng đáng ngờ trên một trang của website. Không rõ liệu ai đó đã truy cập trái phép vào ứng dụng web WordPress hoặc cơ sở dữ liệu MySQL.

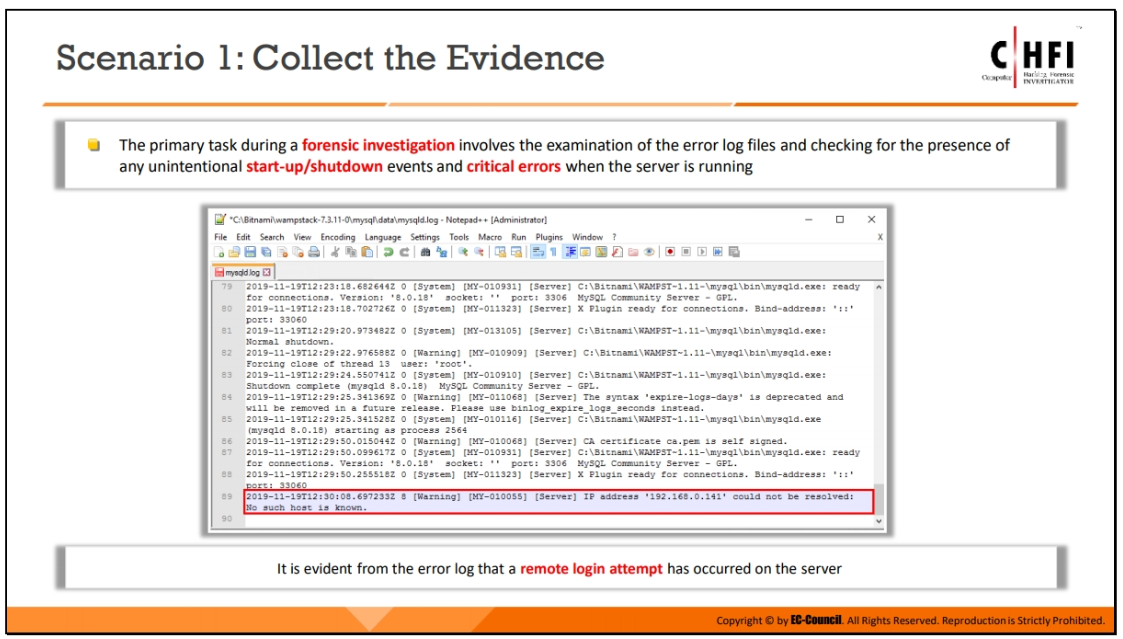
Do đó, chúng tôi đã giải quyết vấn đề bằng hai tình huống, trong đó tình huống đầu tiên liên quan đến việc xác định kẻ tấn công và thu thập tất cả các bài đăng của kẻ tấn công trên trang web WordPress, trong khi kịch bản thứ hai liên quan đến việc khôi phục dữ liệu đã bị xóa.

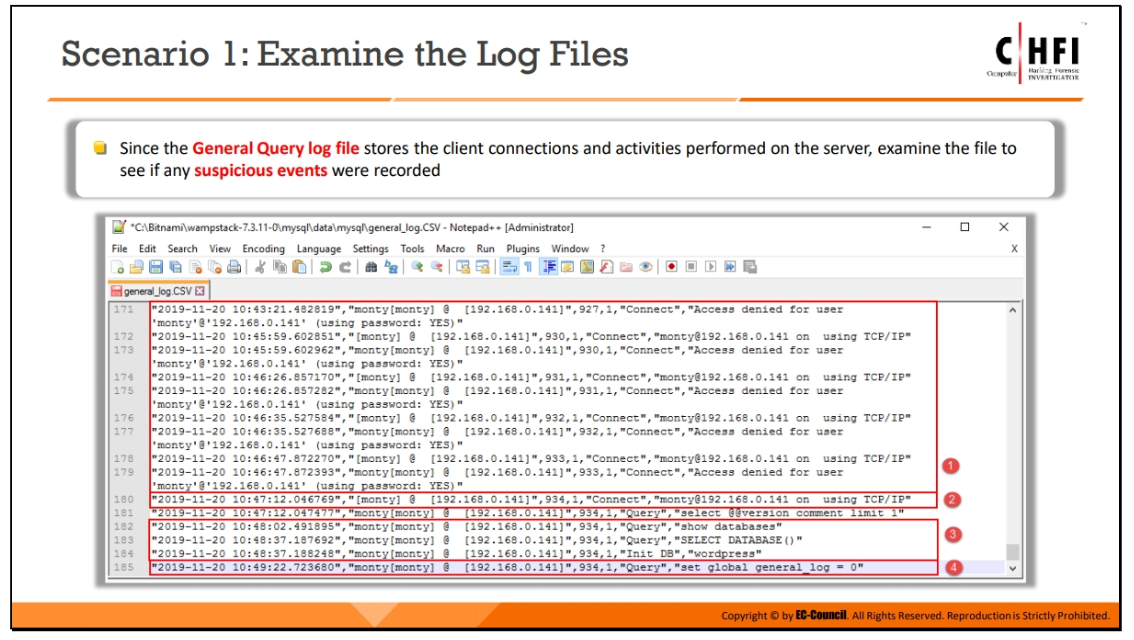


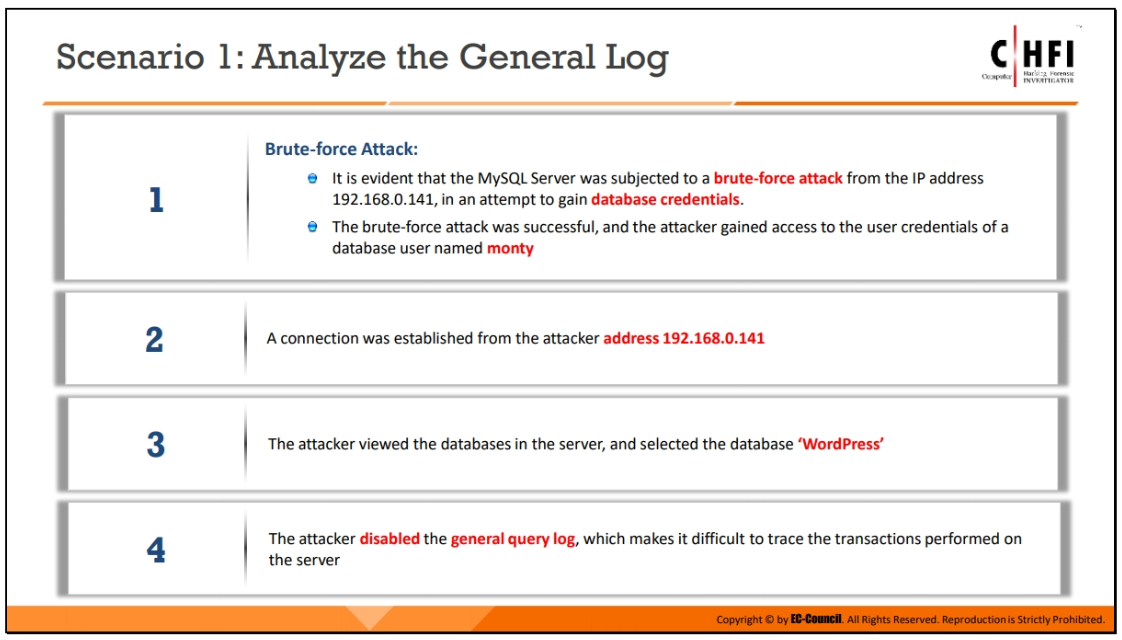
**Điều tra số đối với cở dữ liệu MySQL trang web WordPress : Kịch bản 1**

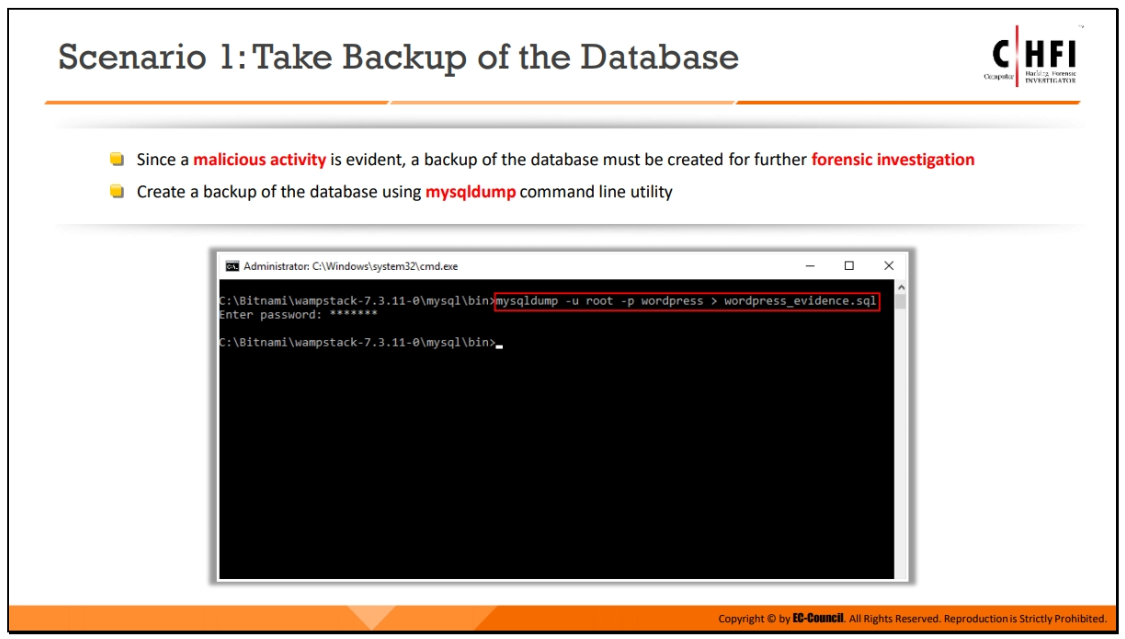
Khi một hoạt động đáng ngờ xảy ra trên cơ sở dữ liệu MySQL của ứng dụng web, nhật ký lỗi và các tệp nhật ký truy vấn chung đóng vai trò là bằng chứng chính để điều tra viên kiểm tra các giao dịch được thực hiện trên cơ sở dữ liệu.

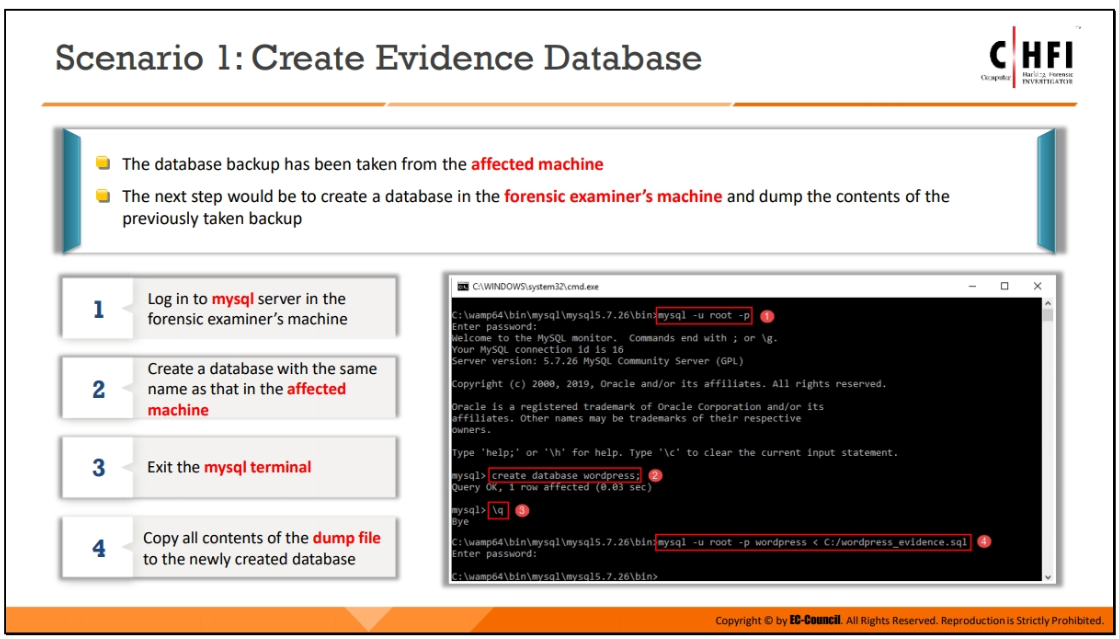
Trong trường hợp này, trước tiên, chúng tôi kiểm tra nhật ký lỗi; sau đó, chúng tôi sẽ phân tích các giao dịch được thực hiện trên cơ sở dữ liệu bằng giao diện ứng dụng dòng lệnh.

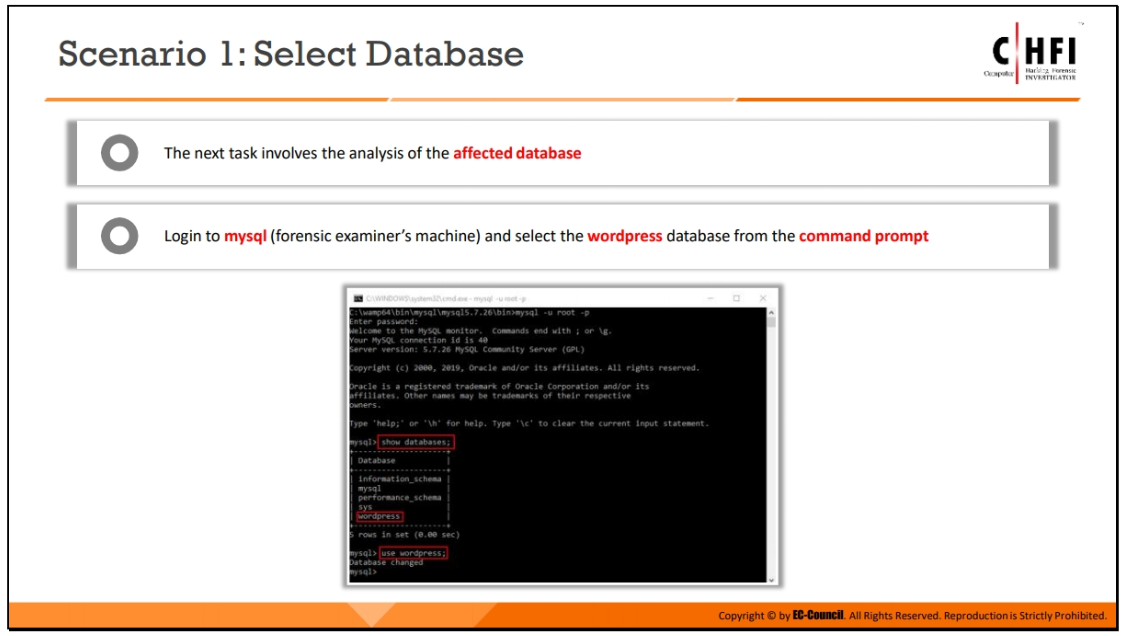


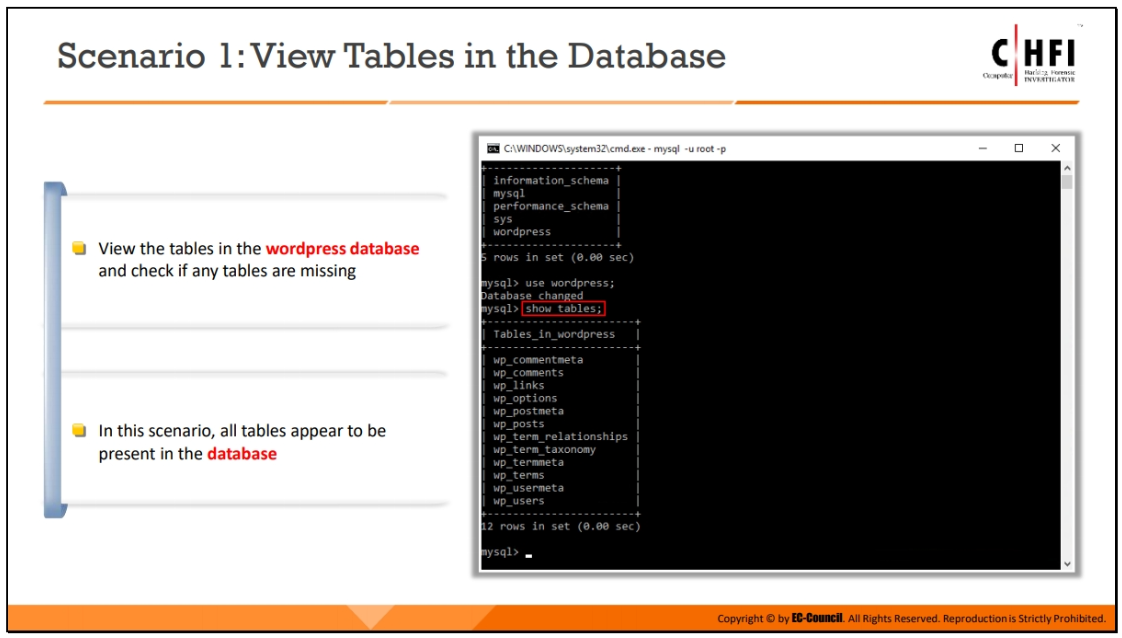


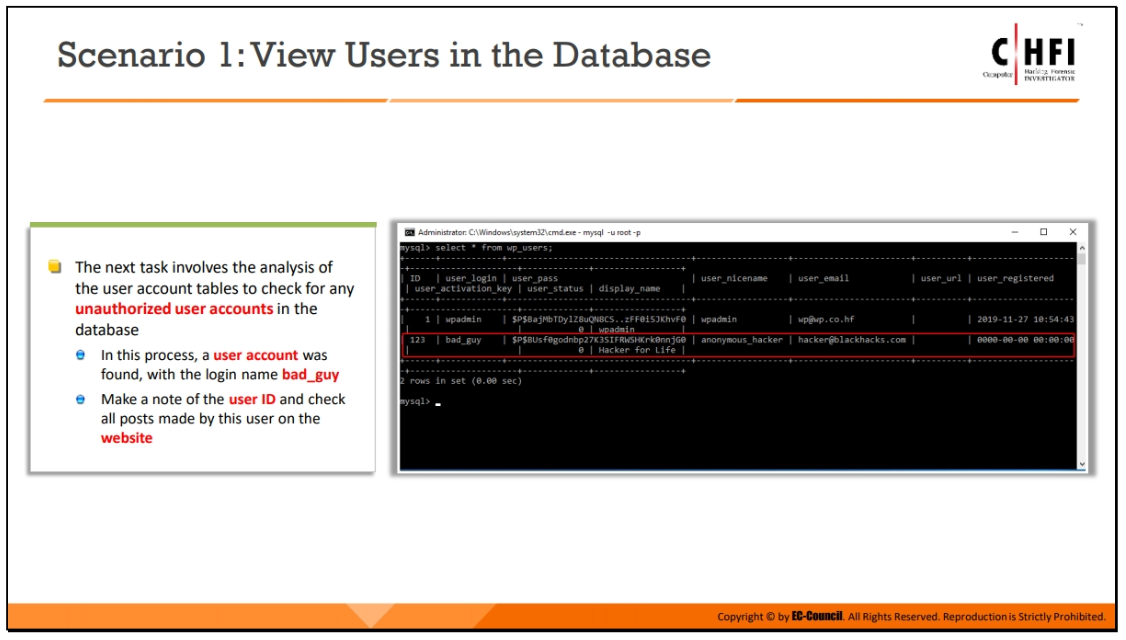


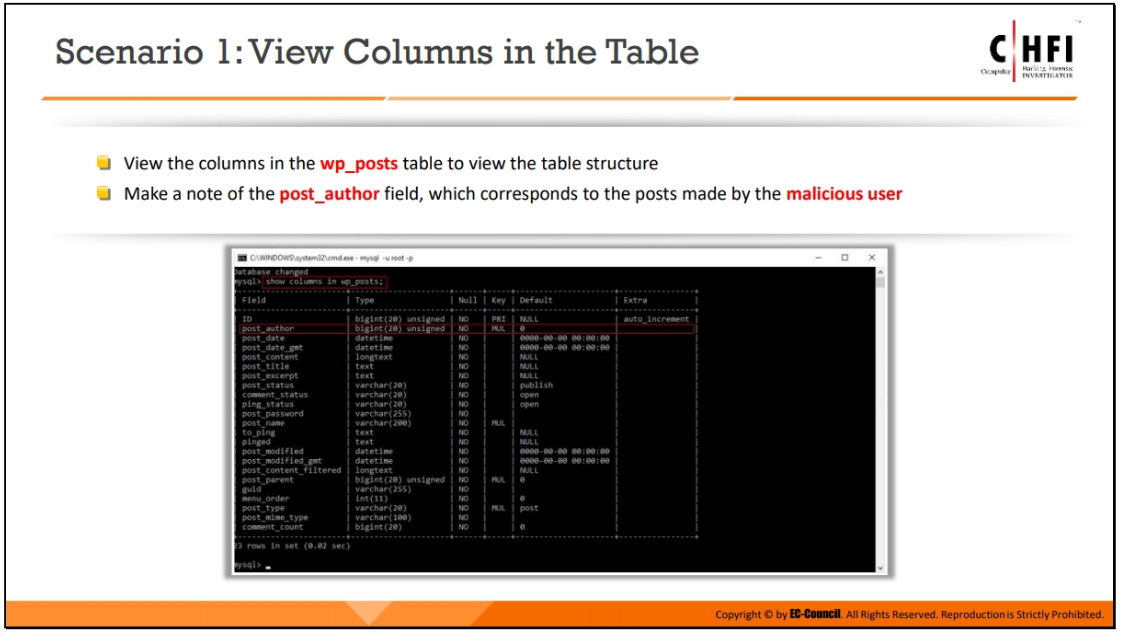


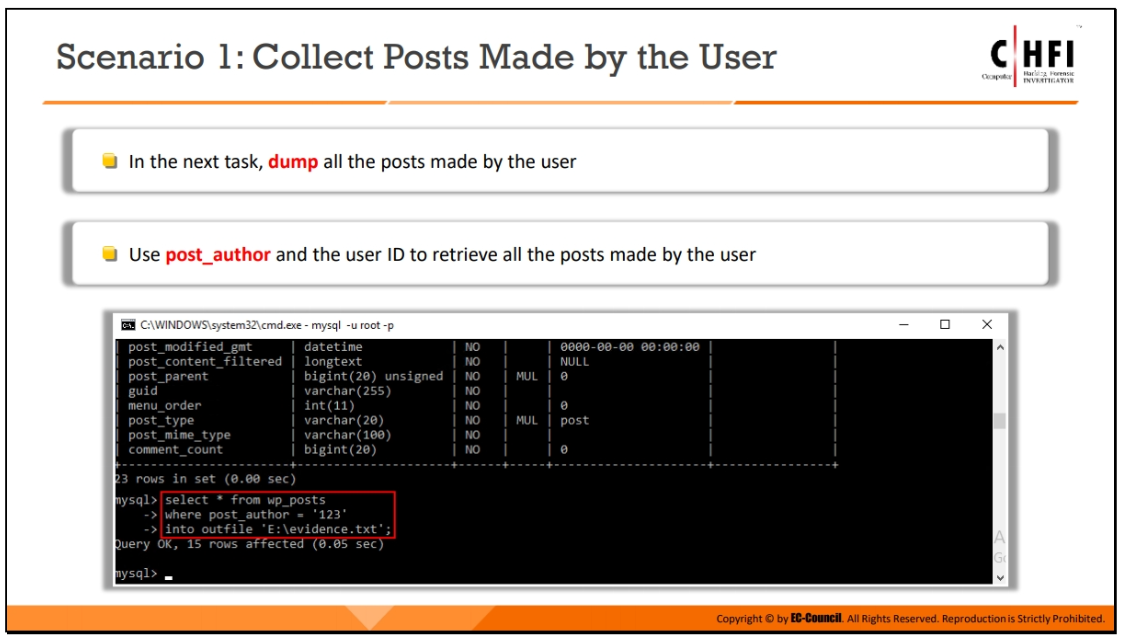


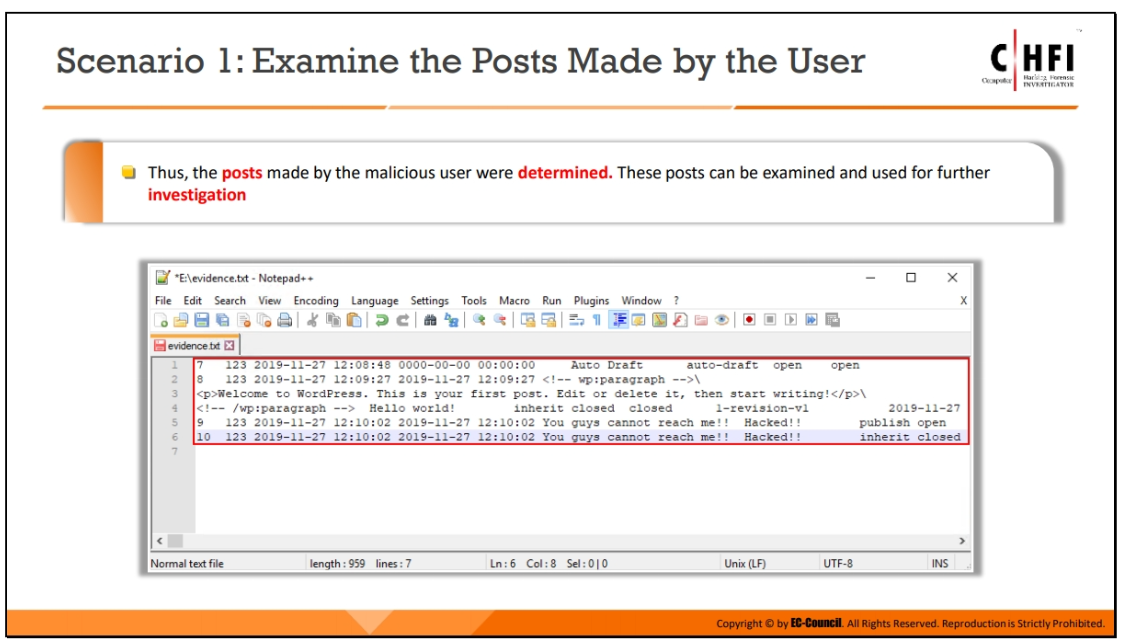








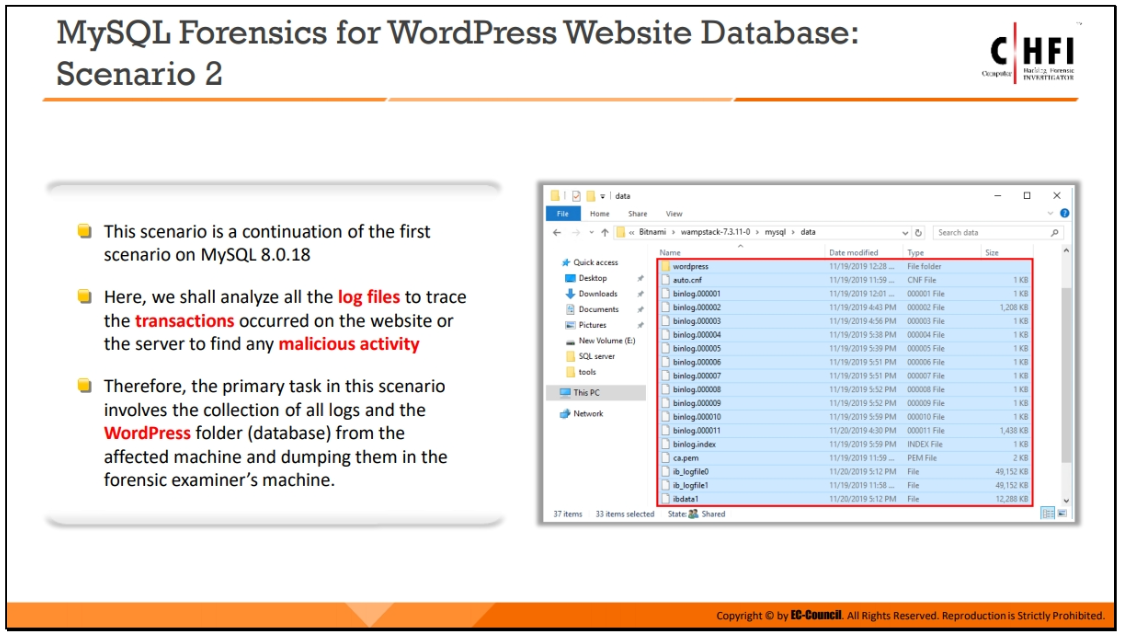




Để tóm tắt kịch bản được trình bày ở trên, kẻ tấn công đã thực hiện một cuộc tấn công brute-forcevào cơ sở dữ liệu MySQL và đã thành công trong việc giành quyền truy cập vào thông tin đăng nhập của người dùng. Sử dụng thông tin xác thực, kẻ tấn công đã đăng nhập vào cơ sở dữ liệu, tạo tài khoản người dùng và vô hiệu hóa truy vấn chung nhật ký. Tắt nhật ký này có nghĩa là MySQL sẽ không thể ghi lại các giao dịch trong tệp nhật ký.

Do đó, như một phần của cuộc điều tra pháp y trên cơ sở dữ liệu MySQL, ứng dụng dòng lệnh đã được sử dụng và một bản sao lưu của cơ sở dữ liệu đã được thực hiện vì các cuộc điều tra số không nên được thực hiện trên máy bị ảnh hưởng. Sau khi hoàn thành, một cơ sở dữ liệu đã được tạo trên máy điều tra và nội dung cơ sở dữ liệu đã được đổ vào nó. Sau đó, ID người dùng của kẻ tấn công được tìm thấy, được sử dụng để xác định các bài đăng của kẻ tấn công trên ứng dụng web.





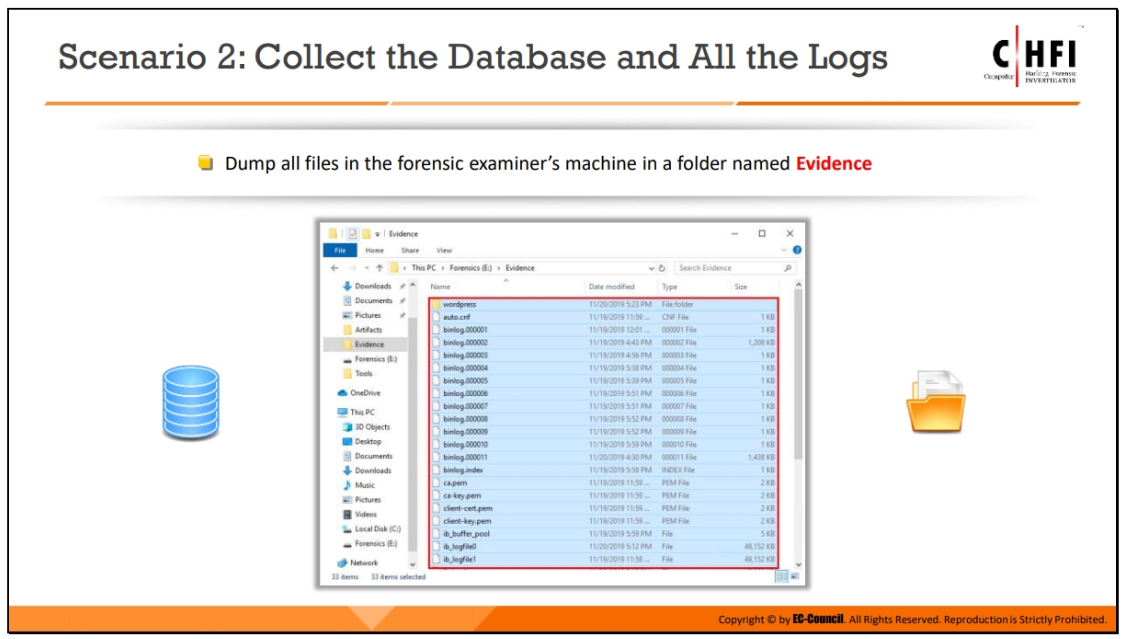
**Điều tra số đối với cở dữ liệu MySQL trang web WordPress : Kịch bản 2**

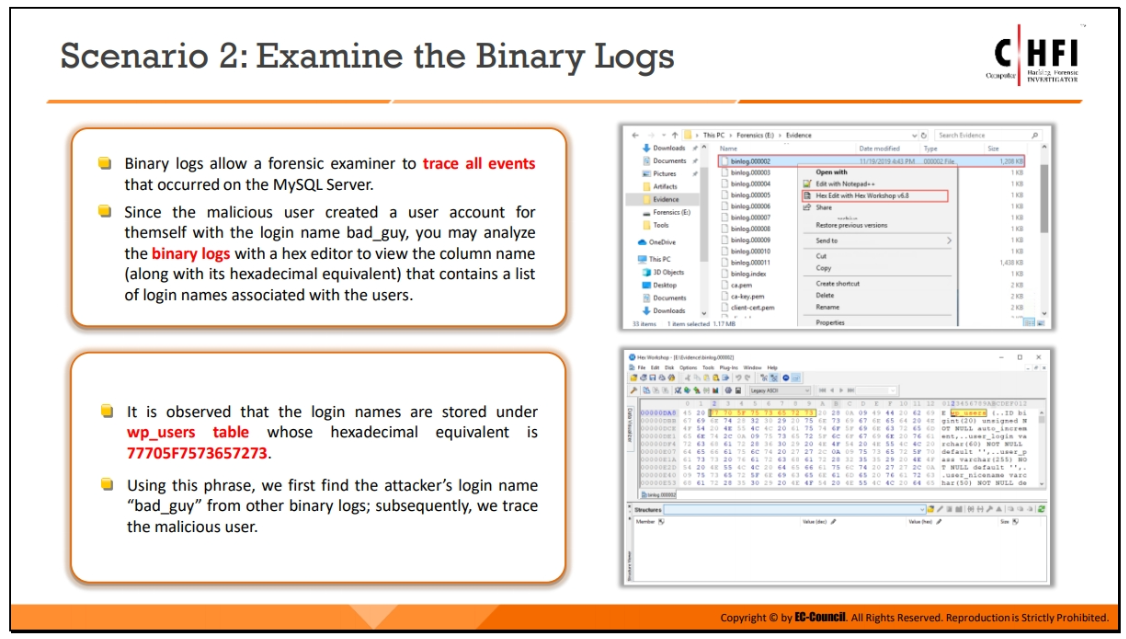
Như đã thảo luận trước đó, MySQL lưu trữ tất cả dữ liệu và giao dịch trong nhiều tệp nhật ký nhị phân. Vì thế, khi ai đó xóa bất kỳ thông tin quan trọng nào một cách cố ý hoặc vô tình, các điều tra viên kiểm tra các tệp nhật ký nhị phân để xem các giao dịch và khôi phục các tệp đã xóa

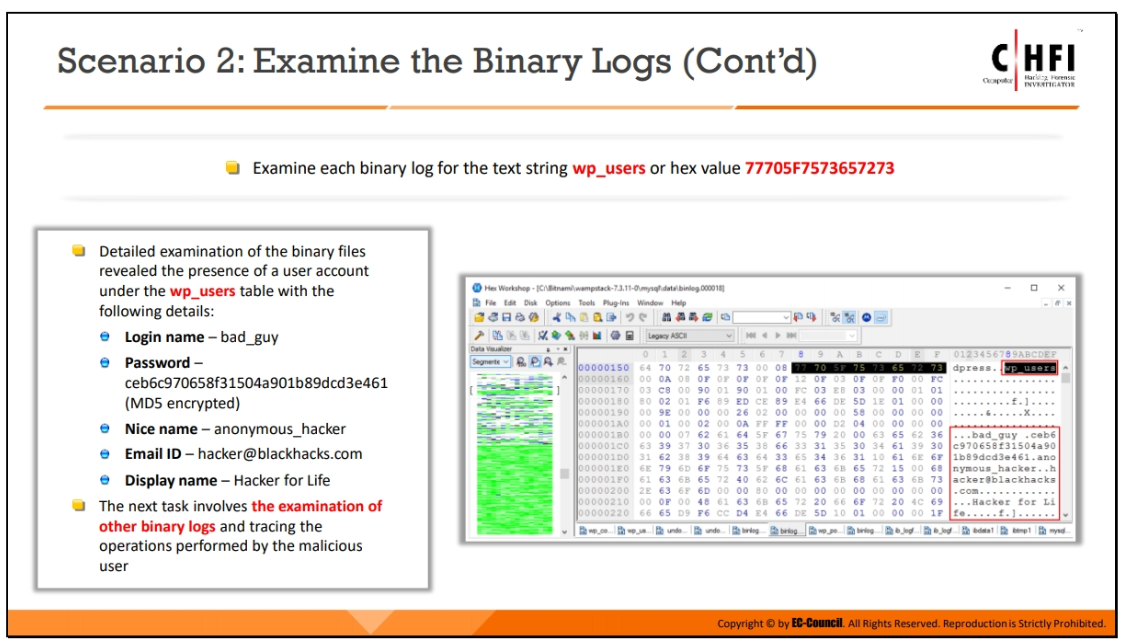
thông tin.

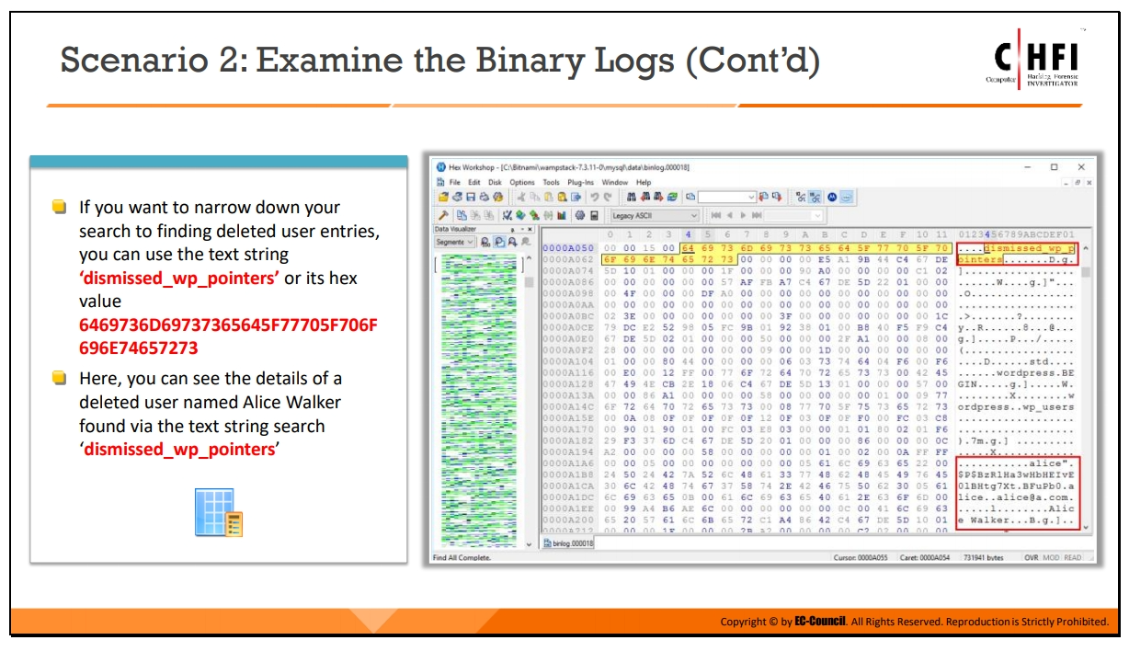
Kịch bản này là phần tiếp theo của kịch bản đầu tiên trên MySQL 8.0.18. Sau đây, chúng tôi sẽ phân tích tất cả các tệp nhật ký để theo dõi các giao dịch xảy ra trên trang web hoặc máy chủ để tìm bất kỳ hoạt động độc hại nào

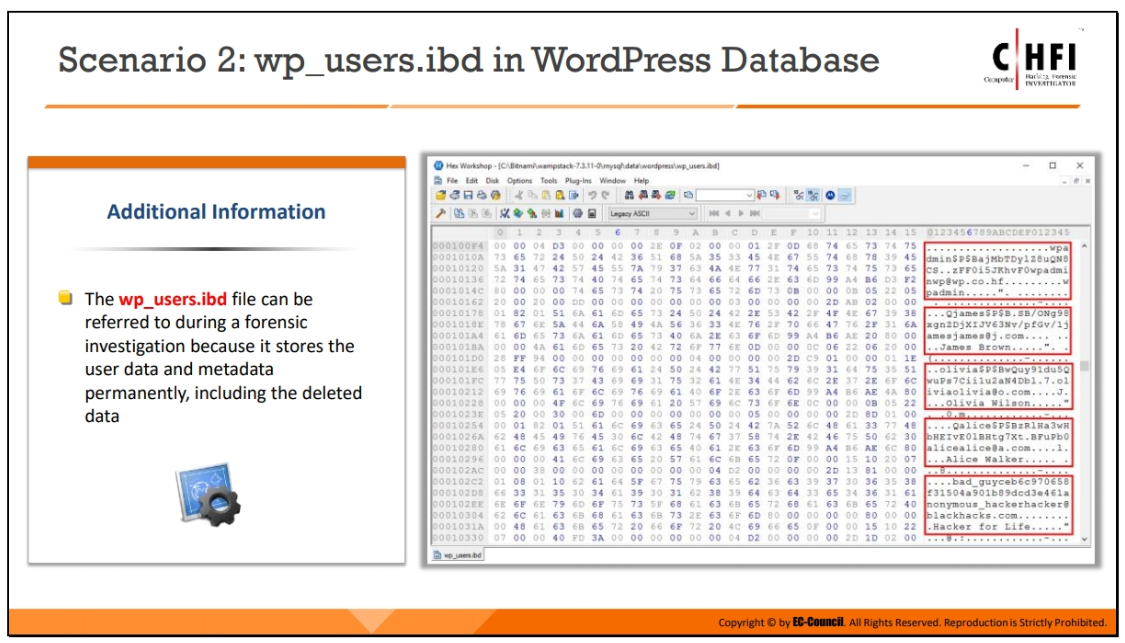
Do đó, nhiệm vụ chính trong kịch bản này liên quan đến việc thu thập tất cả nhật ký và thư mục WordPress (cơ sở dữ liệu) từ máy bị ảnh hưởng và đưa chúng vào máy của điều tra viên.

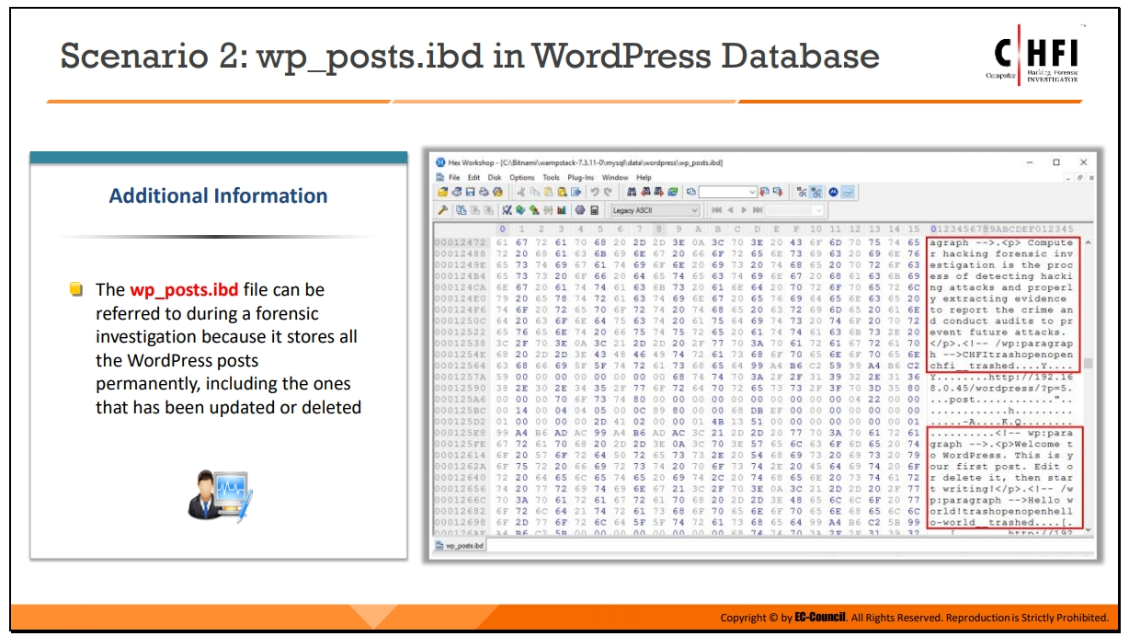




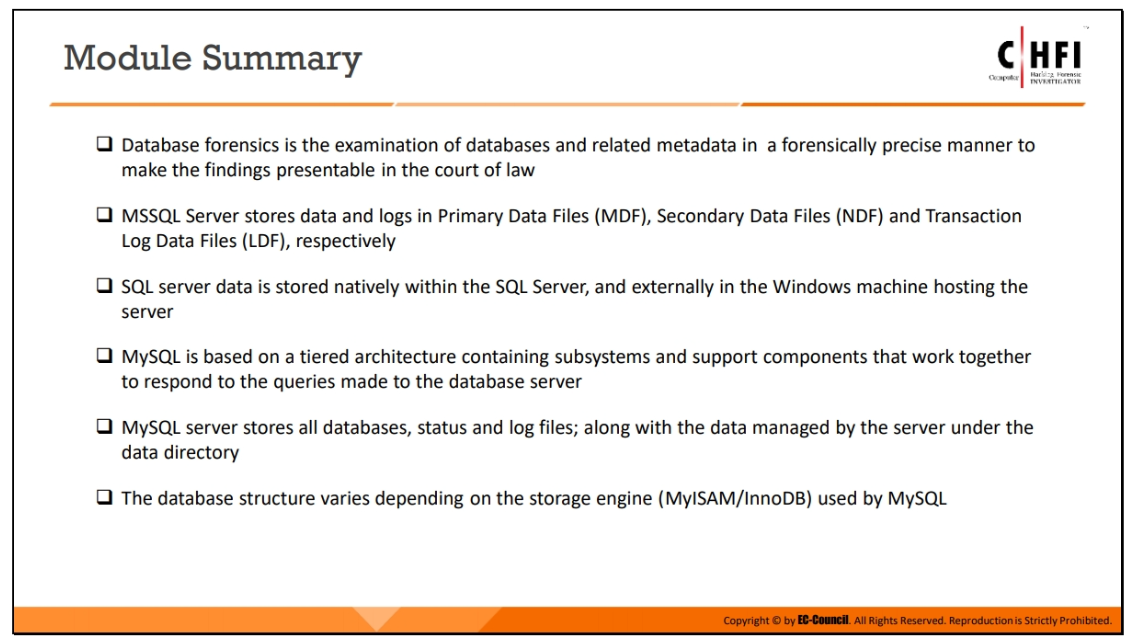








Để tóm tắt kịch bản 2, kẻ tấn công đã tạo một tài khoản người dùng trong cơ sở dữ liệu và đã thao túng nội dung của nó. Do đó, như một phần của cuộc điều tra số trên cơ sở dữ liệu MySQL, chúng tôi đã chuyển tất cả các tệp trong máy điều tra vào một thư mục có tên “Evidence.”. Sau đó, chúng tôi đã mở các tệp nhật ký nhị phân và tìm kiếm chuỗi văn bản “wp\_users”. Sử dụng chuỗi này, truy vấn được thực hiện bởi kẻ tấn công đã được tìm thấy để tạo tài khoản người dùng. Sau đó là các bài viết do kẻ tấn công tạo ra đã được phân tích và chúng tôi có thể thấy rằng kẻ tấn công đã xóa hai bài đăng, các bài đăng này đã được phục hồi. Tệp nhị phân ghi lại các sự kiện cho các mục người dùng cũng đã bị xóa. Ngoài ra, đã tìm thấy các tệp wp\_user.ibd và wp\_posts.ibd lưu trữ dữ liệu liên quan đến tài khoản người dùng (cùng với những tài khoản đã bị xóa) và các bài đăng trên WordPress. Các điều tra viên có thể tham khảo các tệp này như một phần của cuộc điều tra số. Vì vậy, chúng tôi đã kiểm tra các tệp nhật ký nhị phân và xác định được các bài đăng và người dùng bị xóa.



**Tổng kết**

Trong mô-đun này, chúng ta đã thảo luận về hai loại hệ thống quản lý cơ sở dữ liệu, MSSQL và MySQL, cùng với cấu trúc tệp cơ bản và kho lưu trữ bằng chứng của chúng. Điều tra viên có thể thực hiện các kỹ thuật được nhắc đến trong mô-đun này để điều tra quản lý cơ sở dữ liệu các hệ thống. Họ có thể khôi phục các mục đã xóa, tìm các giao dịch được thực hiện trong cơ sở dữ liệu (MSSQL và MySQL), tạo bản sao lưu của các tệp cơ sở dữ liệu (MySQL) và phân tích chúng.

Các điểm nổi bật chính của mô-đun này đã được đưa ra dưới đây:

* Điều tra cơ sở dữ liệu là việc kiểm tra cơ sở dữ liệu và siêu dữ liệu quan trọng một cách chính xác để làm bằng chứng có thể trình bày tại tòa án của pháp luật.
* Máy chủ MSSQL lưu trữ dữ liệu và ghi nhật ký trong tệp dữ liệu chính (MDF), tệp dữ liệu thứ cấp (NDF) và tệp dữ liệu nhật ký giao dịch (LDF), tương ứng.
* Dữ liệu máy chủ SQL được lưu trữ nguyên bản trong máy chủ SQL và bên ngoài máy chủ Windows.
* MySQL dựa trên kiến ​​trúc tầng chứa các hệ thống con và các thành phần hỗ trợ hoạt động cùng nhau để phản hồi các truy vấn được thực hiện cho máy chủ cơ sở dữ liệu.
* Máy chủ MySQL lưu trữ tất cả các cơ sở dữ liệu, trạng thái và tệp nhật ký; cùng với dữ liệu được quản lý bởi máy chủ dưới dữ liệu trực tiếp.
* Cấu trúc cơ sở dữ liệu khác nhau tùy thuộc vào công cụ lưu trữ (MyISAM/InnoDB) được sử dụng bởi MySQL.