

# THU THẬP THIẾT BỊ ĐIỆN TỬ TRÊN PHƯƠNG TIỆN BỊ CHÁY TRONG CÁC VỤ TAI NẠN GIAO THÔNG

HOÀNG TRỌNG LỰC\*

*Hiện nay, việc thu thập các thiết bị điện tử trên phương tiện bị cháy do tai nạn giao thông chưa được chú trọng, chưa khai được nhiều thông tin, dấu vết từ các thiết bị điện tử được thu thập. Bài viết làm rõ phương pháp thu thập thiết bị điện tử trên phương tiện bị cháy do tai nạn giao thông nhằm khai thác, khôi phục dữ liệu đảm bảo yêu cầu phục vụ hoạt động điều tra các vụ cháy.*

*Từ khóa: Thu thập dấu vết cháy, khám nghiệm hiện trường tai nạn giao thông, thu thập thiết bị điện tử bị cháy, thiết bị điện tử.*

*Ngày nhận bài: 15/8/2022; Biên tập xong: 06/9/2022; Duyệt đăng: 02/10/2022*

Currently, the collection of electronic devices on vehicles burned in traffic accidents has not been paid much attention that leads to information and traces from the collected electronic devices have been disclosed. The article clarifies the method of collecting electronic devices on vehicles burned in traffic accidents in order to exploit and recover data to meet the requirements for fire investigation activities.

**Keywords:** Collecting fire traces, examining traffic accident scenes, collecting burnt electronics, electronic equipment.

**T**hực tế, để xác định nguyên nhân do tai nạn gây cháy hay do cháy gây tai nạn giao thông (TNGT) cần dựa vào nhiều nguồn thông tin, dấu vết, vật chứng như: Dấu vết tại hiện trường, dấu vết trên phương tiện, dấu vết xung quanh hiện trường, đặc biệt là dữ liệu điện tử trên các phương tiện điện tử được gắn trên phương tiện tham gia giao thông. Thiết bị điện tử là nơi chứa nhiều thông tin, dữ liệu, dấu vết có giá trị xác định nguyên nhân cháy, nguyên nhân tai nạn và các tình tiết khác của vụ việc đã xảy ra cần được thu thập, khai thác hiệu quả. Trên các phương tiện giao thông thường có các thiết bị điện tử như: Thiết bị giám sát hành trình (hộp đen); camera hành trình; điện thoại di động. Trong đó:

*Hộp đen* là thiết bị giám sát, lưu trữ toàn bộ hành trình di chuyển của phương tiện, thời điểm dừng, đỗ, tốc độ, cảnh báo nguy hiểm... Vị trí lắp đặt của hộp đen thường được kết nối trực tiếp vào hệ thống điện trên xe. Việc thu thập thiết bị này được thực hiện tương đối dễ dàng, chỉ cần tìm tháo

các vị trí kết nối hộp đen với phương tiện rồi tiến hành thu giữ, bảo quản như với dấu vết, vật chứng thông thường hoặc sao chép dữ liệu trực tiếp trong hộp đen bằng phần mềm TachoMetter có kết nối máy tính qua mạch RS 232 sẽ thu được hiệu quả.

*Điện thoại di động:* Khi phát hiện điện thoại di động trên phương tiện bị cháy trên phương tiện, cần thu thập và tìm kiếm dữ liệu liên quan đến vụ TNGT thông qua thẻ nhớ và dữ liệu trong bộ nhớ của máy. Để phục hồi, trích xuất, thu thập dữ liệu điện tử của bộ nhớ trong điện thoại di động có thể sử dụng các thiết bị chuyên dụng UFED, XRY... để sao lưu dữ liệu từ điện thoại sang máy tính để phục hồi và đọc dữ liệu trong điện thoại di động như: hình ảnh, hành trình, video clip...

*Camera hành trình:* Thiết bị này có chức năng ghi lại những âm thanh, hình ảnh khi xe di chuyển và lưu trong thẻ nhớ. Có thể đọc dữ liệu trực tiếp trên màn hình

*\* Phó Giáo sư, Tiến sĩ, Phó Trưởng khoa Kỹ thuật hình sự, Học viện Cảnh sát nhân dân*

camera hoặc qua cổng HDMI cho phép kết nối hình ảnh sang màn hình khác. Trường hợp dữ liệu bị xóa, ghi đè có thể dùng các thiết bị khôi phục dữ liệu.

Trong thực tế, các thiết bị điện tử bị cháy được thu thập ở trên phương tiện giao thông thường là thiết bị kỹ thuật số, có chip điện tử hay thẻ nhớ... Đa số các thiết bị này trong tình trạng không thể hoạt động, hệ thống cơ học của thiết bị điện tử bị hư hỏng, máy đọc dữ liệu không nhận diện được ổ cứng, thẻ nhớ, USB, không phát hiện được thiết bị điện tử. Điều này xảy ra khi hệ thống “bản mạch in” (Printed Circuit Board) hay PCB của ổ cứng bị lỗi, hỏng. Giám định viên chỉ có thể khôi phục dữ liệu trong các thiết bị này bằng cách duy nhất là thay bảng mạch in cùng loại với thiết bị. Việc thay bảng mạch in rất phức tạp, đòi hỏi người thực hiện phải được đào tạo một cách chuyên sâu. Sau khi thay thế bảng mạch, thông thường thiết bị sẽ hoạt động và hệ thống phương tiện, máy tính sẽ nhận diện, thu thập được dữ liệu. Những thiết bị điện tử thu thập được xác định hỏng một số bộ phận thì cần thay thế những bộ phận tương ứng, đúng chủng loại để phương tiện hoạt động được thì mới tiến hành thu thập dữ liệu lưu trữ trong những thiết bị này. Việc tháo, lắp và thay thế các bộ phận trên thiết bị thu thập cần có những dụng cụ chuyên dụng và phải được thực hiện bởi những chuyên gia về phục hồi dữ liệu. Sau khi thay thế xong, giám định viên sẽ tiến hành kiểm tra đánh giá khả năng hoạt động của thiết bị được thay thế. Sau khi đã xác nhận thiết bị hoạt động đảm bảo, sẽ tiến hành sao lưu và khôi phục dữ liệu như bình thường.

Quá trình khôi phục dữ liệu điện tử trong các thiết bị điện tử bị cháy thực tế rất phức tạp, tiềm ẩn nhiều nguy cơ mất dữ liệu hoặc phá hủy phương tiện điện tử đã thu thập, nhưng nếu không thực hiện thì cơ quan điều tra sẽ không thể có được dữ liệu từ những thiết bị này. Do vậy, việc

tiến hành đọc, khôi phục, thu thập dữ liệu trên các thiết bị điện tử bị hỏng, cháy trong hiện trường TNGT cần phải được tiến hành một cách thận trọng, tỉ mỉ, thậm chí đặt ra tình huống chấp nhận rủi ro khi việc sửa chữa, thay thế không hiệu quả. Trong khuyến cáo, cần xác định chỉ được thực hiện khi không còn phương pháp nào khác để đọc, khôi phục, thu thập dữ liệu từ các thiết bị này. Khôi phục, trích xuất dữ liệu trong các thiết bị điện tử bị cháy cần được tính toán chính xác, đảm bảo đủ các điều kiện thực hiện thu thập tối ưu thông tin có trong thiết bị điện tử này. Thực tế cho thấy, trong nhiều vụ việc dữ liệu điện tử trong các thiết bị này là chứng cứ duy nhất để khẳng định nguyên nhân các vụ TNGT, các thông tin được khai thác phục vụ rất hiệu quả cho hoạt động điều tra các vụ TNGT như: Hành trình di chuyển, biến kiểm soát, nhận dạng người tham gia giao thông, nhận diện người cầm lái, thời điểm xảy ra tai nạn, diễn biến trước, trong và sau khi tai nạn... Từ đó, làm căn cứ cho cơ quan Cảnh sát điều tra xác định nguyên nhân chính xác do TNGT dẫn đến cháy hay do các thiết bị điện tử bị cháy dẫn đến TNGT và các vấn đề cần chứng minh khác.

Để kịp thời khắc phục những hạn chế, nâng cao hiệu quả khai thác, khôi phục dữ liệu điện tử bị cháy trên phương tiện trong các vụ TNGT, cần hoàn thiện một số giải pháp sau đây:

**Một là**, chuẩn hóa lực lượng tham gia khám nghiệm hiện trường tai nạn giao thông, khám nghiệm phương tiện, thu thập dữ liệu điện tử.

Theo quy định, chủ thể thu thập thiết bị điện tử bị cháy trên phương tiện giao thông được giao cho 04 lực lượng gồm: Cơ quan Cảnh sát điều tra, lực lượng Kỹ thuật hình sự, lực lượng Cảnh sát giao thông và lực lượng Cảnh sát phòng cháy, chữa cháy và cứu nạn, cứu hộ. Mặc dù đã có sự phân cấp tương đối rõ ràng, nhưng

thực tế lại bất cập bởi lực lượng Kỹ thuật hình sự là lực lượng có chuyên môn về thu thập thiết bị điện tử, khám nghiệm phương tiện, khám nghiệm hiện trường lại không được tiếp cận hiện trường ngay từ ban đầu. Một số vụ việc do các lực lượng khác chưa đủ chuyên môn dẫn đến bế tắc, hư hỏng, không thể khai thác dữ liệu trong các thiết bị khi đó mới trưng cầu cơ quan giám định, khôi phục dữ liệu. Do vậy, đa số các thiết bị điện tử bị cháy trên phương tiện trong các vụ TNGT đa số hỏng rất nặng, rất khó sửa chữa để khôi phục dữ liệu phục vụ hoạt động điều tra. Trên cơ sở đó, cần rà soát các văn bản pháp luật để chỉnh sửa theo hướng giao trách nhiệm thu thập thiết bị điện tử bị cháy trên phương tiện, khám nghiệm hiện trường TNGT cho lực lượng Kỹ thuật hình sự thực hiện, lực lượng này phải có mặt ngay từ ban đầu khi xảy ra TNGT. Đồng thời, do tính chất các vụ TNGT có xảy ra cháy thường gây hậu quả rất nghiêm trọng, các thiết bị điện tử bị cháy rất khó khai thác dữ liệu nên việc thu thập các thiết bị điện tử, khám nghiệm hiện trường TNGT trong những trường hợp này phải có mặt của giám định viên về cháy, nổ và giám định viên về kỹ thuật số, điện tử để thu thập, khôi phục dữ liệu điện tử nhằm xác định nguyên nhân cháy.

*Hai là*, khi thu thập thiết bị điện tử cần quan tâm thu thập các tài liệu, dấu vết, vật chứng khác để bổ trợ, làm tăng giá trị pháp lý cho “chứng cứ điện tử”.

Để điều tra làm rõ nguyên nhân và các vấn đề cần chứng minh trong vụ việc mang tính hình sự, cần dựa vào nhiều nguồn thông tin, dấu vết vật chứng. Đối với những vụ TNGT có phương tiện, thiết bị điện tử bị cháy ngoài các thiết bị điện tử phải thu thập cũng cần thu thập các nguồn chứng cứ khác như: Lấy lời khai, tài liệu liên quan đến mật khẩu, dấu vết đường vân, dấu vết cơ học, dấu vết cháy, dấu vết sinh học, dấu vết kỹ thuật và những thiết bị điện tử ở những khu vực khác có kết

nối các thiết bị đã thu thập và liên quan đến hiện trường TNGT...

Cán bộ thu thập thiết bị điện tử và giám định viên có thể bị triệu tập tại phiên tòa để trình bày về quá trình thu thập, khôi phục dữ liệu điện tử trong các thiết bị điện tử đã thu thập. Vì vậy, khi tiến hành các phương pháp, phương tiện thực hiện việc thu thập thiết bị và khôi phục dữ liệu điện tử phải ghi chép, quay video khi thực hiện để làm căn cứ chứng minh tính khách quan của những dữ liệu đã được thu thập. Đảm bảo tính nguyên vẹn của chứng cứ khi trình bày tại Tòa án, những trường hợp thiết bị điện tử bị cháy, hỏng thì việc ghi nhận một cách khách quan và có thể kiểm chứng là nguyên tắc phải làm khi thực hiện thu thập dữ liệu điện tử. Nếu tòa án yêu cầu giám định viên thực hiện việc phục hồi, tìm kiếm chứng cứ điện tử lưu trong thiết bị điện tử đã thu thập thì kết quả thu thập được trước tòa cũng phải tương tự như kết quả đã trình bày trước đó.

Đối với các thiết bị điện tử bị cháy việc khôi phục dữ liệu là vô cùng khó khăn, trường hợp khôi phục được dữ liệu cần nhanh chóng sao chép sang ổ đĩa khác và in tất cả các dữ liệu đã tìm thấy ra giấy, lập biên bản quá trình thực hiện thu giữ có sự chứng kiến của những người liên quan. Bởi lẽ, có nhiều trường hợp những thiết bị điện tử này bị hỏng, bị phá hủy sau khi giám định viên đã đọc, khôi phục, gây khó khăn trong việc thực hiện lại các thao tác thu thập, khôi phục dữ liệu như ban đầu.

*Ba là*, bồi dưỡng kiến thức chuyên môn cho lực lượng tham gia khám nghiệm phương tiện tai nạn giao thông đảm bảo trình độ khi thực hiện nhiệm vụ.

Thu thập thiết bị điện tử đòi hỏi cán bộ ngoài kiến thức về dấu vết hình sự cần có kiến thức về công nghệ thông tin, am hiểu về các thiết bị điện tử thì mới có thể đảm bảo việc thu thập thiết bị điện tử không

làm mất dữ liệu và không làm ảnh hưởng đến các dấu vết khác. Việc không đảm bảo kiến thức chuyên môn trong khám nghiệm hiện trường sẽ gặp khó khăn trong tiến hành các hoạt động phát hiện, thu thập, khôi phục dữ liệu điện tử phục vụ điều tra, giải quyết bản chất vụ việc.

Theo khảo sát, đa số cán bộ khám nghiệm hiện trường hiện nay về cơ bản đã đáp ứng kiến thức về công tác khám nghiệm hiện trường. Tuy nhiên, những kiến thức chuyên sâu về nghiệp vụ thu thập thiết bị điện tử còn rất hạn chế nên có nhiều vụ việc thu thập thiết bị điện tử và thiết bị điện tử bị cháy trong các vụ TNGT không đảm bảo yêu cầu, gây khó khăn cho công tác phát hiện, khôi phục dữ liệu điện tử, ảnh hưởng đến hoạt động điều tra. Do vậy, cần tổ chức các lớp tập huấn, đào tạo ngắn hạn từ 03 đến 06 tháng về các nội dung liên quan đến quy trình khám nghiệm hiện trường TNGT, khám nghiệm phương tiện; quy trình thu thập thiết bị điện tử; quy trình xử lý thiết bị điện tử bị hỏng, cháy; quy trình khôi phục dữ liệu điện tử... Về lâu dài, cần bổ sung các nội dung về dữ liệu điện tử, phương tiện điện tử, khám nghiệm phương tiện vào chương trình đào tạo cho sinh viên chuyên ngành Kỹ thuật hình sự trong các trường Công an nhân dân. Hơn nữa, về công tác cán bộ cần quan tâm bổ sung nguồn nhân lực được đào tạo chuyên môn về điện, điện tử, công nghệ thông tin... ở các trường đại học ngoài ngành làm công tác chuyên môn này.

**Bốn là**, trang bị, nâng cấp các phương tiện, thiết bị hỗ trợ thu thập, trích xuất và khôi phục dữ liệu điện tử từ các thiết bị điện tử chuyên dụng.

Các phương tiện, công cụ, phần mềm được sử dụng trong thu thập dữ liệu điện tử thường là những phương tiện, phần mềm mà Việt Nam chưa đủ năng lực để nghiên cứu, sản xuất, mà phải nhập ngoại với giá thành rất cao. Do vậy, cần rà soát, nghiên cứu xây dựng đầu tư trang thiết bị tổng thể với lộ trình đầu tư hợp lý, đảm

bảo các phương tiện hiện đại luôn đáp ứng được các yêu cầu thực tế. Đồng thời, việc trang bị các thiết bị hiện đại phải đi đôi với việc tăng cường khai thác tối đa tính năng, tác dụng của từng thiết bị đã được trang cấp. Trong thu thập dữ liệu điện tử cần được trang bị những thiết bị như: Thiết bị UFED, XRAY... là thiết bị có khả năng truy cập sâu vào dữ liệu thiết bị di động bằng cách kết hợp các kiểu trích xuất dữ liệu; giúp khôi phục cả dữ liệu bị xóa, ẩn với khả năng mạnh mẽ. Hệ thống phục hồi dữ liệu trên thiết bị di động PC 3000 Mobile, đây là loại công cụ chuyên nghiệp để khôi phục dữ liệu điện tử từ các thiết bị di động bị hỏng như: Điện thoại di động thông minh, máy tính bảng... Thiết bị này cho phép khôi phục nội dung và khôi phục hệ thống tệp và có tính năng phân tích sâu và phục hồi các hệ thống tập tin bị hỏng một cách hợp lý. Ngoài ra, để thu thập, phân tích hiệu quả dữ liệu trên điện thoại di động có thể trang bị thêm các phương tiện hỗ trợ khác như hệ thống máy tính có cấu hình cao, máy in, máy ảnh, máy quay...

Chương trình phần mềm khôi phục, phân tích dữ liệu là phần mềm có khả năng phục hồi dữ liệu (Data recover), khôi phục dữ liệu lưu trữ khi không thể truy cập được bằng cách thông thường do bị xóa (delete), định dạng cài đặt, ghi đè... sử dụng một số phần mềm như: Encase, Magnet, OS Forensic, Xry.../.

## TÀI LIỆU THAM KHẢO

1. Viện Khoa học hình sự, Cục Cảnh sát Phòng cháy chữa cháy và CNCH; *Báo cáo tổng kết công tác năm 2021*, Hà Nội.
2. Lương Khắc Vọng (2015), *Phát hiện, thu thập, đánh giá dấu vết cháy trong điều tra các vụ án cháy theo chức năng của lực lượng cảnh sát phòng cháy và chữa cháy*, Luận án Tiến sĩ Luật, Học viện Cảnh sát nhân dân, Hà Nội
3. Hoàng Trọng Lực (2021), *Khám nghiệm hiện trường cháy nhà cao tầng theo chức năng của lực lượng kỹ thuật hình sự Công an nhân dân*, Đề tài cấp bộ, V04 – Bộ Công an