

HƯỚNG DẪN MỘT SỐ KỊCH BẢN SỬ DỤNG TRONG PHẦN MỀM MTA MOBILE FORENSIC

1. Kịch bản 1: Điều tra số trên thiết bị di động Android

1.1. Mô tả kịch bản

1.1.1. Kịch bản

Sau một thời gian đấu tranh phòng chống tội phạm sử dụng công nghệ cao, Bộ Quốc phòng đã tiến hành điều tra và bắt giữ nghi phạm. Tang vật thu giữ bao gồm một thiết bị di động Android cùng với mật khẩu mà đối tượng đã khai báo. Sau đó, Bộ Quốc phòng đã bàn giao thiết bị di động và giao cho Học viện Kỹ thuật Quân sự điều tra, phân tích dữ liệu và báo cáo về Bộ Quốc phòng.

1.1.2. Các bước tiến hành

Bước 1. Tiếp nhận thiết bị: Học viện Kỹ thuật Quân sự tiếp nhận thiết bị di động Android và mật khẩu. Giao cho cơ quan chức năng tiến hành kiểm tra ban đầu để đảm bảo thiết bị còn nguyên vẹn và không có dấu hiệu can thiệp hoặc thay đổi từ bên ngoài sau khi bị thu giữ.

Bước 2. Sao lưu dữ liệu thiết bị: Sử dụng các công cụ điều tra số chuyên dụng MTA Mobile Forensic để trích xuất toàn bộ dữ liệu từ thiết bị. Dữ liệu được sao lưu bao gồm tin nhắn, cuộc gọi, tệp phương tiện, lịch sử duyệt web, dữ liệu ứng dụng, và các thông tin hệ thống... Bản sao này được lưu trữ an toàn để phục vụ cho quá trình phân tích và điều tra.

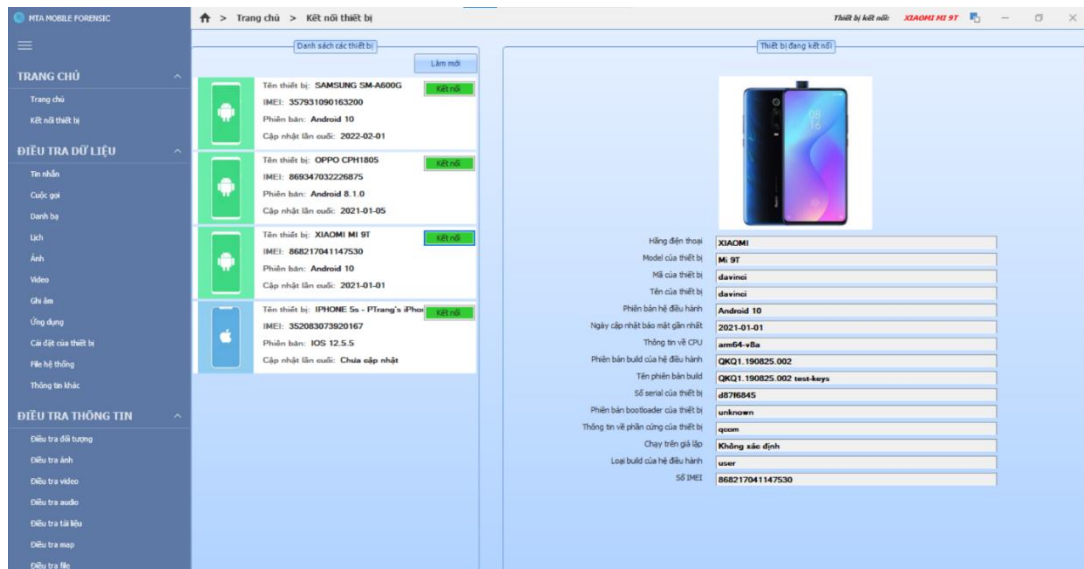
Bước 3. Điều tra dữ liệu thiết bị: Tiến hành phân loại và phân tích toàn bộ dữ liệu thu thập được, đặc biệt chú trọng đến các tệp tin, ứng dụng, và hoạt động đáng ngờ có thể liên quan đến hành vi phạm tội. Xem xét chi tiết lịch sử liên lạc qua các phương tiện như cuộc gọi, tin nhắn và mạng xã hội để xác định mối liên hệ với các đối tượng liên quan. Ngoài ra, tiến hành điều tra dữ liệu ảnh, video và vị trí địa lý kèm theo để làm rõ hành trình di chuyển và các hoạt động của đối tượng.

Bước 4. Báo cáo dữ liệu thu được: Tổng hợp các kết quả phân tích và tạo báo cáo chi tiết về các bằng chứng kỹ thuật số thu được từ thiết bị. Báo cáo sẽ nêu rõ các hoạt động đáng ngờ, dữ liệu quan trọng, và các kết luận hỗ trợ cho quá trình

điều tra. Báo cáo này được gửi về Bộ Quốc phòng để phục vụ quá trình truy tố và xử lý đối tượng.

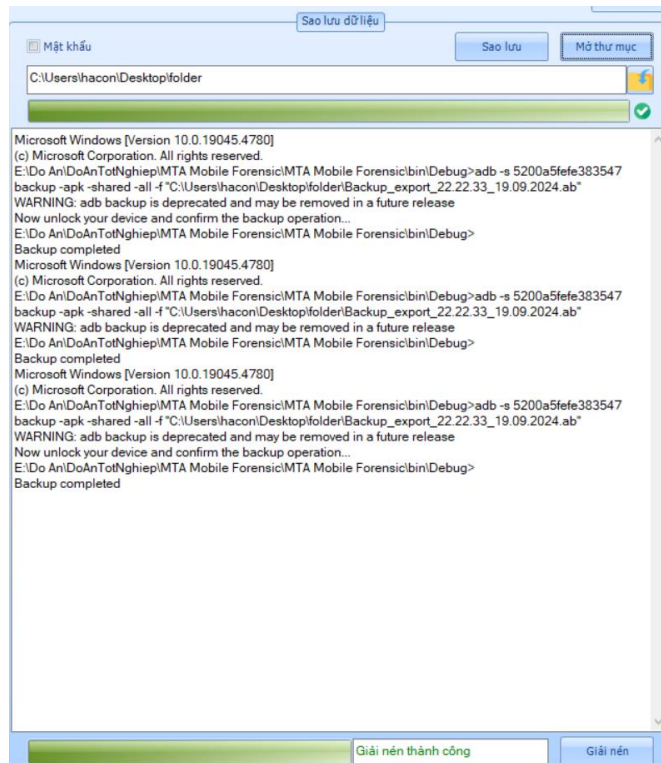
1.2. Thứ tự hành động

Bước 1: Tiếp nhận và kết nối thiết bị: Người điều tra tiếp nhận thiết bị và kết nối thiết bị với công cụ điều tra số MTA Mobile Forensic.



Hình 4.1. Kết nối với thiết bị để điều tra

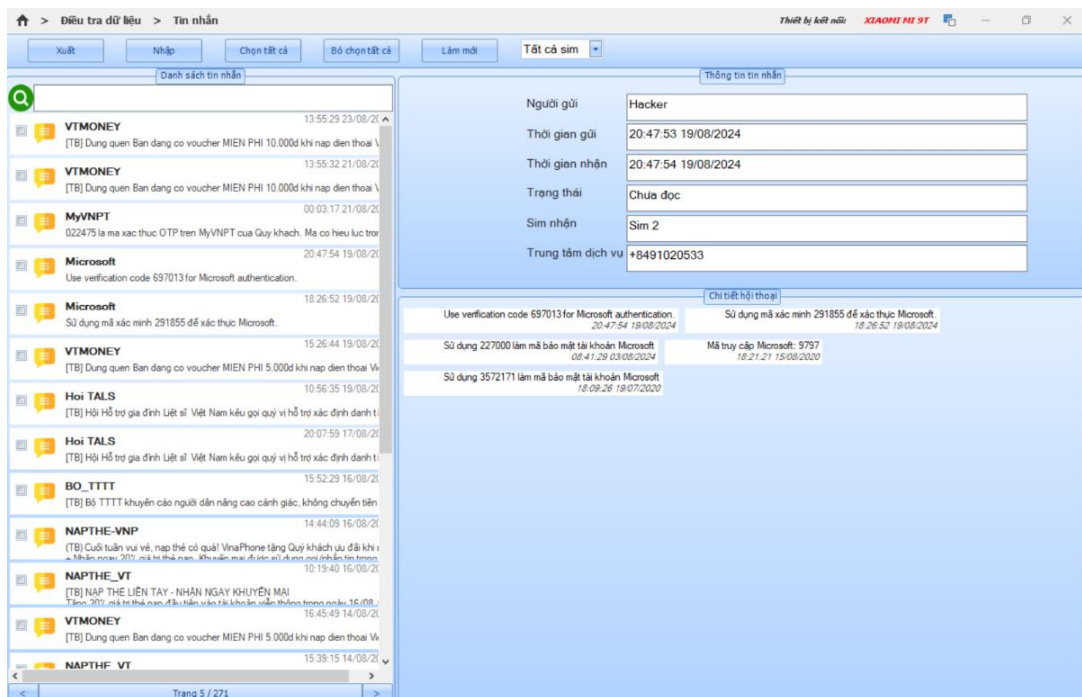
Bước 2: Sao lưu dữ liệu: Người điều tra vào chức năng sao lưu dữ liệu để sao lưu dữ liệu từ thiết bị, đồng thời có 1 bản backup để có thể phục hồi dữ liệu khi cần thiết.



Hình 4.2. Sao lưu dữ liệu thiết bị di động Android

Bước 3: Phân tích dữ liệu

- Tìm kiếm và phân tích dữ liệu tin nhắn trên thiết bị:



Hình 4.3. Điều tra dữ liệu tin nhắn

- Tìm kiếm và phân tích dữ liệu danh bạ trên thiết bị:

Điều tra dữ liệu > Danh bạ

Thiết bị kết nối: XIAOMI MI 9T

Xuất Nhập Chọn tất cả Bỏ chọn tất cả Làm mới Tất cả

Danh bạ

097 832 40 98

A Quang Tân Hoa
097 908 04 09

A Tuấn TTG
097 927 05 82

Manh Hao
097 412 7917

Bác Tuấn
097 282 6126

Manh Hao
097 412 7917

Hoàng
097 455 5939

Bằng Lxe
097 872 9445

Cường
097 936 5963

K42 Vương A
098 155 45 99

Cô Huyền Bếp
098 265 81 75

Bác Minh
098 338 94 06

Em Hiếu Như Thanh
098 404 00 94

A Việt Nam

Thông tin chi tiết

Tên danh bạ: Đại lý Hunter Coin Cấp 1

Số điện thoại: 097 927 05 82

Công ty: Không có

Lưu tại: Tài khoản Google

Tài khoản: hacongquocun@gmail.com

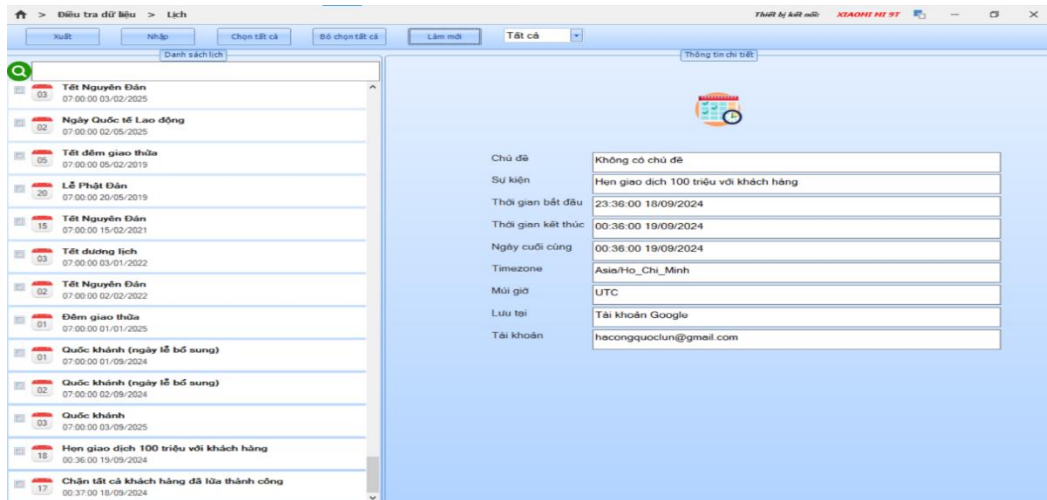
Nickname: Không có

Cập nhật lần cuối: 06:05:46 15/09/2024

Mã bấm: 3cKJhpJKOY+UvHerhXkhh5iyQh0=

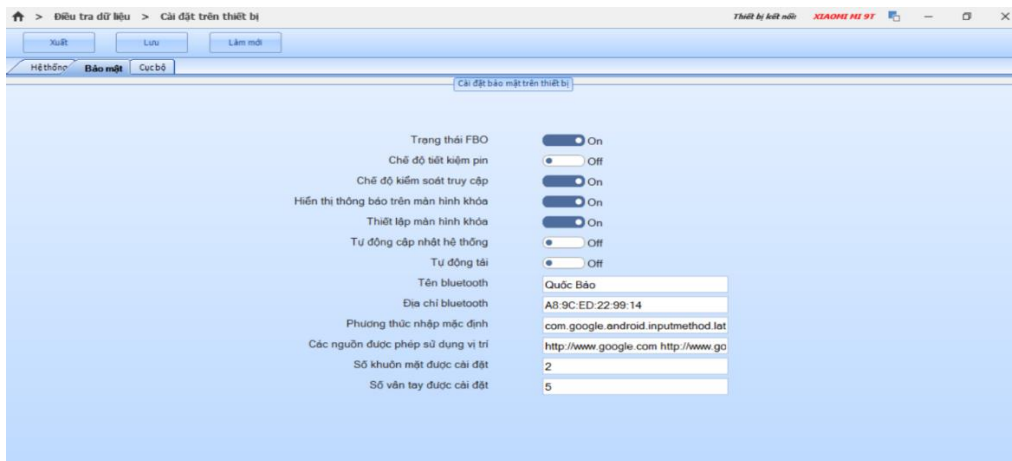
Hình 4.4. Điều tra dữ liệu danh bạ

- Tìm kiếm và phân tích dữ liệu lịch trên thiết bị:



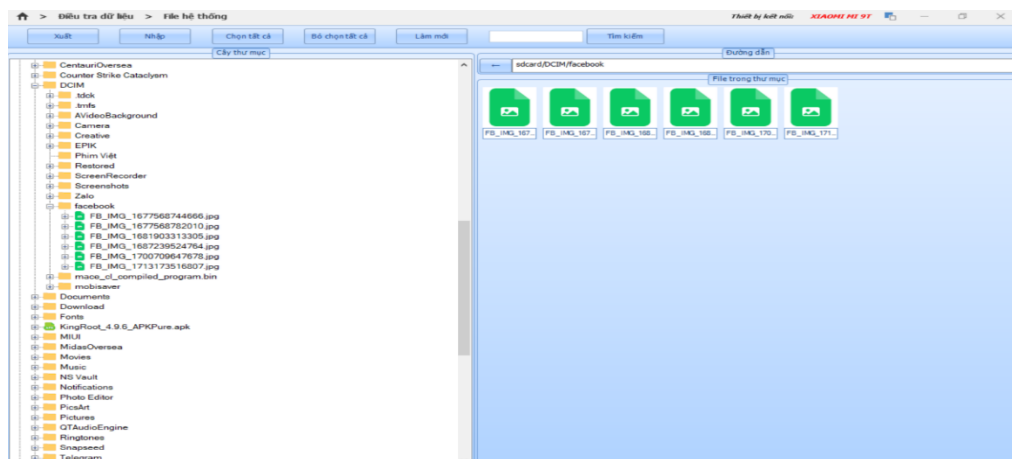
Hình 4.5. Điều tra dữ liệu lịch

- Tìm kiếm và phân tích thông tin cài đặt trên thiết bị:



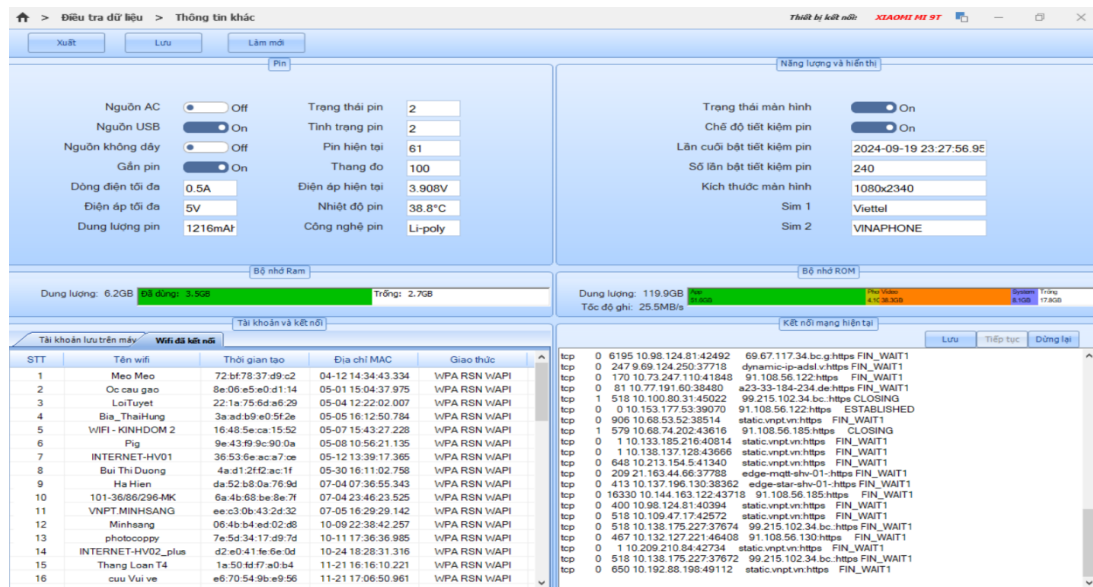
Hình 4.6. Điều tra dữ liệu cài đặt của thiết bị

- Tìm kiếm và phân tích dữ liệu file hệ thống trên thiết bị:



Hình 4.7. Điều tra file hệ thống của thiết bị

- Tìm kiếm và phân tích thông tin khác trên thiết bị:



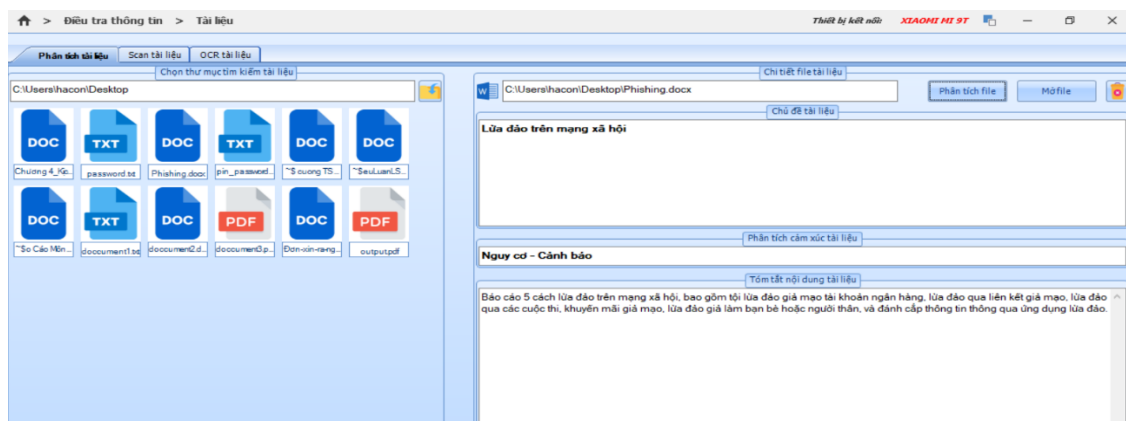
Hình 4.8. Điều tra thông tin khác trên thiết bị

- Tìm kiếm và phân tích các tài khoản, wifi đã kết nối trên thiết bị:

Tài khoản và kết nối			
Tài khoản lưu trên máy		Wifi đã kết nối	
STT	Tên tài khoản	Tên ứng dụng	
1	hacongquoc***@gmail.com	com.google	
2	hacongquoc***@gmail.com	com.google	
3	6230***535	com.xiaomi	
4	WPS***ice	cn.wps.moffice	
5	Zalo***ount	com.zing.zalo	
6	Ti***k	com.ss.android.ugc.trill	
7	5280***196	org.telegram.messenger	
8	7165***172	org.telegram.messenger	
9	Mes***ger	com.facebook.messenger	
10	100011***265424	com.facebook.auth.login	
11	7193***114	www.instagram.com	

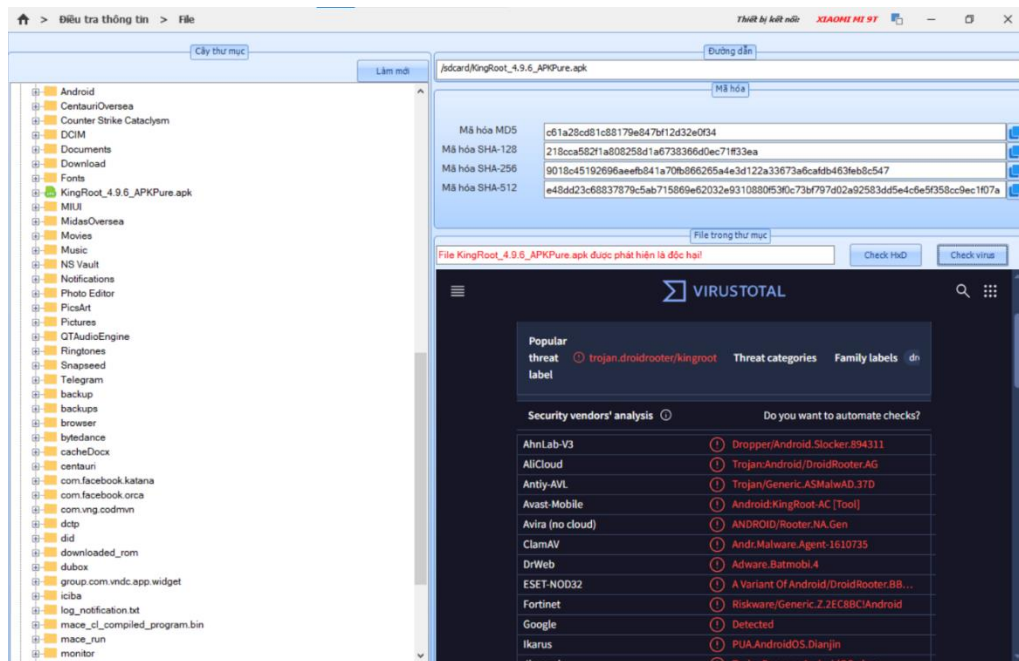
Hình 4.9. Điều tra các tài khoản và wifi đã kết nối

- Tìm kiếm và phân tích các nội dung tài liệu trên thiết bị



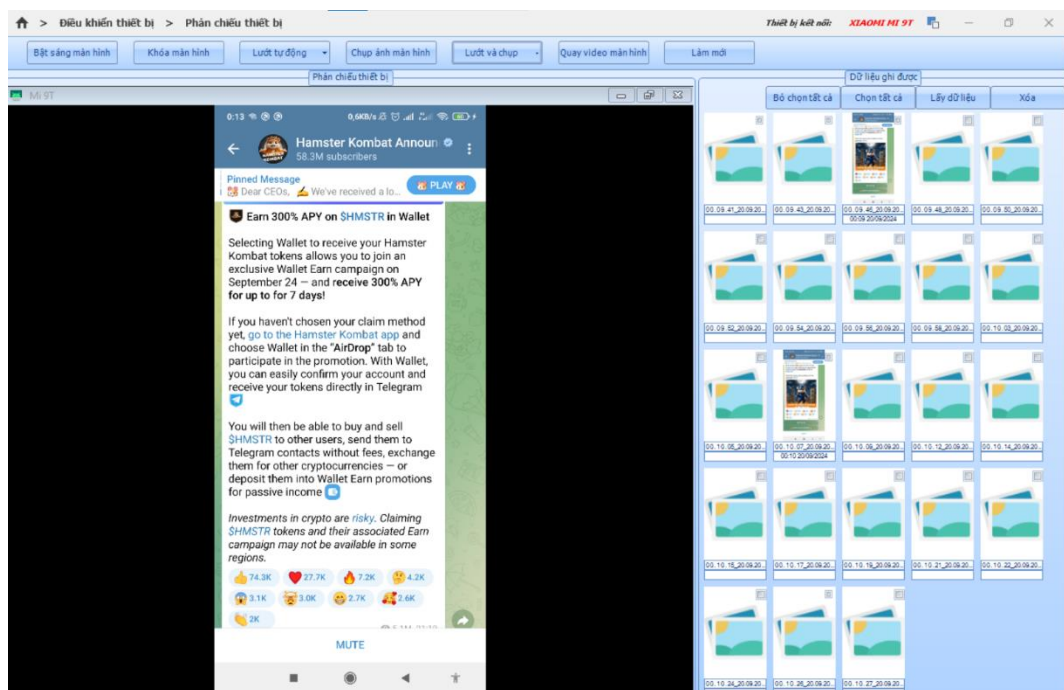
Hình 4.10. Tìm kiếm và phân tích nội dung tài liệu

- Phân tích các tệp tin nghi ngờ độc hại trên thiết bị:



Hình 4.11. Phân tích tệp tin nghi ngờ độc hại

- Điều tra và ghi lại bằng chứng những nội dung quan trọng:



Hình 4.12. Lưu lại những chứng cứ quan trọng

Bước 4: Tạo báo cáo điều tra: Người điều tra tạo báo cáo về kết quả điều tra dữ liệu trên thiết bị:

TỔ CHỨC ... CƠ QUAN ...	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc					
Hà Nội, ngày 10 tháng 9 năm 2024						
BÁO CÁO KẾT QUẢ ĐIỀU TRA SỐ						
Trên thiết bị: Xiaomi MI9T						
Người thực hiện điều tra: Hà Công Quốc Bảo						
Thời gian phiên điều tra: 10 giờ 10 phút, ngày 10 tháng 9 năm 2024						
Số serial thiết bị: 5200a5fefe383547						
Thư mục sao lưu: E:\Backup_Android\Backup_export_10.09.2024						
Tập dữ liệu sao lưu: E:\Backup_Android\Backup_5200a5fefe383547.ab						
KẾT QUẢ THỰC HIỆN ĐIỀU TRA:						
1. Dữ liệu tin nhắn:						
STT	Loại tin nhắn	Người gửi	Người nhận	Nội dung	Thời gian	Sim
1	Nhận	Nguyễn Văn A (0987654321)	Thiết bị	Đã hoàn thành theo kế hoạch đề ra	2023-11-20 10:30:00	1
2	Gửi	Thiết bị	Nguyễn Văn A (0987654321)	Tiến độ của vụ việc thế nào rồi?	2023-11-20 10:25:00	1

Hình 4.13. Báo cáo kết quả phiên điều tra

2. Kịch bản 2: Điều tra số trên thiết bị di động IOS

2.1. Mô tả kịch bản

2.1.1. Kịch bản

Trong cuộc trấn áp bạo loạn lật đổ của một nhóm đối tượng tại địa bàn, phân đội trực chiến của Học viện Kỹ thuật Quân sự đã bắt giữ thành công kẻ cầm đầu, đồng thời thu giữ một thiết bị di động sử dụng hệ điều hành iOS. Qua quá trình điều tra, đối tượng đã hợp tác và cung cấp mật khẩu khóa màn hình của thiết bị. Học viện sau đó đã yêu cầu các cơ quan chức năng tiến hành điều tra, phân tích dữ liệu liên quan từ thiết bị này đồng thời báo cáo kết quả về Học viện.

2.1.2. Các bước tiến hành

Bước 1. Tiếp nhận thiết bị: Các cơ quan chức năng tiến hành tiếp nhận và kiểm tra sơ bộ để đảm bảo thiết bị vẫn còn nguyên trạng, không có bất kỳ dấu hiệu thay đổi hay can thiệp từ bên ngoài.

Bước 2. Sao lưu dữ liệu: Sử dụng công cụ điều tra số MTA Mobile Forensic để sao chép và điều tra toàn bộ dữ liệu từ thiết bị. Các loại dữ liệu được

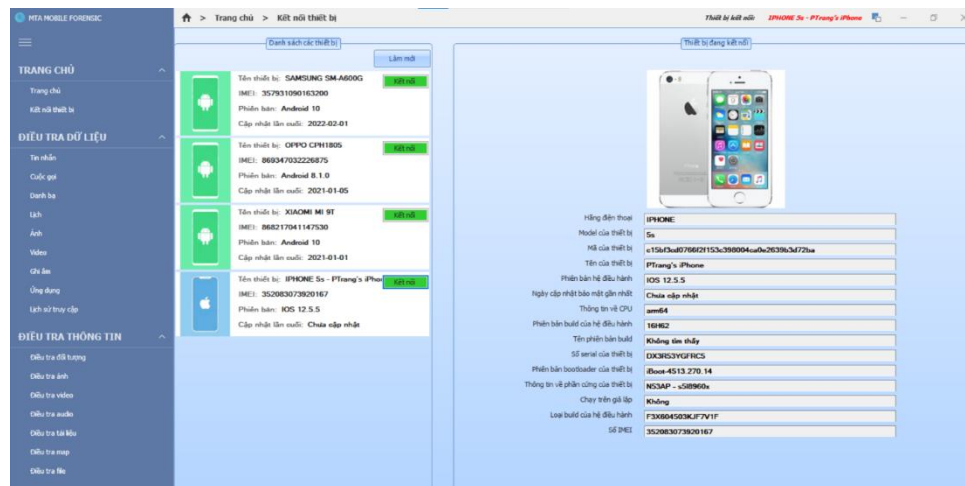
sao lưu bao gồm tin nhắn, nhật ký cuộc gọi, tệp tin đa phương tiện, lịch sử trình duyệt, dữ liệu ứng dụng và thông tin hệ thống. Bản sao lưu này sẽ được lưu trữ để phục vụ cho quá trình phân tích và điều tra.

Bước 3. Phân tích dữ liệu: Thực hiện việc phân loại và phân tích toàn diện các dữ liệu đã thu thập, tập trung vào những tệp tin, ứng dụng, và hoạt động có khả năng liên quan đến hành vi phạm pháp. Các thông tin liên lạc như tin nhắn, cuộc gọi, ảnh, video và ghi âm nhằm xác định các mối quan hệ với các đối tượng liên quan. Dữ liệu về hình ảnh, video và vị trí địa lý cũng sẽ được điều tra để làm rõ hành vi và lộ trình di chuyển của đối tượng.

Bước 4. Lập báo cáo: Tổng hợp kết quả phân tích và xây dựng báo cáo chi tiết về những chứng cứ kỹ thuật số thu thập được từ thiết bị. Báo cáo sẽ bao gồm những hoạt động nghi vấn, thông tin quan trọng và các kết luận hỗ trợ cho quá trình điều tra.

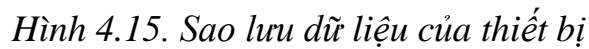
2.2. Thứ tự hành động

Bước 1: Tiếp nhận và kết nối thiết bị: Người điều tra tiếp nhận thiết bị và kết nối thiết bị với công cụ điều tra số MTA Mobile Forensic.

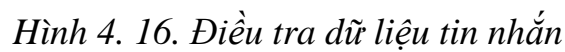


Hình 4.14. Kết nối thiết bị để điều tra

Bước 2: Sao lưu dữ liệu: Người điều tra vào chức năng sao lưu dữ liệu để sao lưu dữ liệu từ thiết bị, đồng thời có 1 bản backup để có thể phục hồi dữ liệu khi cần thiết.



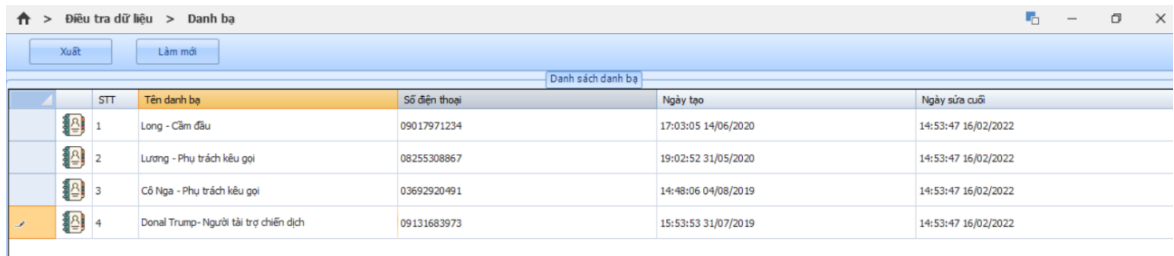
- Tìm kiếm và phân tích dữ liệu tin nhắn trên thiết bị:



- Tìm kiếm và phân tích dữ liệu cuộc gọi trên thiết bị:

Hình 4.17. Điều tra dữ liệu cuộc gọi

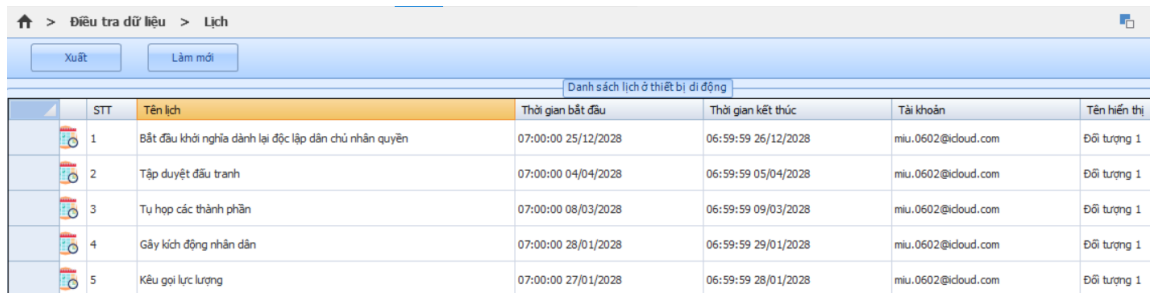
- Tìm kiếm và phân tích dữ liệu danh bạ trên thiết bị:



STT	Tên danh bạ	Số điện thoại	Ngày tạo	Ngày sửa đổi
1	Long - Cầm đầu	09017971234	17:03:05 14/06/2020	14:53:47 16/02/2022
2	Lương - Phụ trách kêu gọi	08255308867	19:02:52 31/05/2020	14:53:47 16/02/2022
3	Cô Nga - Phụ trách kêu gọi	03692920491	14:48:06 04/08/2019	14:53:47 16/02/2022
4	Donald Trump- Người tài trợ chiến dịch	09131683973	15:53:53 31/07/2019	14:53:47 16/02/2022

Hình 4.18. Điều tra dữ liệu danh bạ

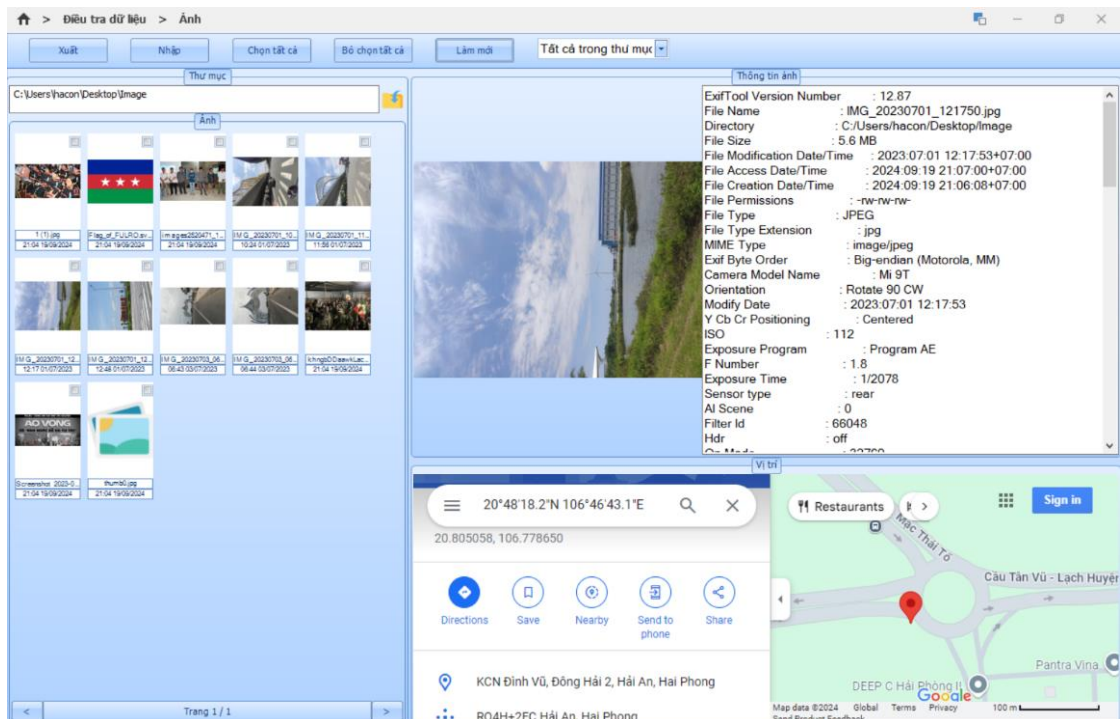
- Tìm kiếm và phân tích dữ liệu lịch trên thiết bị:



STT	Tên lịch	Thời gian bắt đầu	Thời gian kết thúc	Tài khoản	Tên hiển thị
1	Bắt đầu khởi nghĩa dành lại độc lập dân chủ nhân quyền	07:00:00 25/12/2028	06:59:59 26/12/2028	miu.0602@icloud.com	Đối tượng 1
2	Tập duyệt đấu tranh	07:00:00 04/04/2028	06:59:59 05/04/2028	miu.0602@icloud.com	Đối tượng 1
3	Tụ họp các thành phần	07:00:00 08/03/2028	06:59:59 09/03/2028	miu.0602@icloud.com	Đối tượng 1
4	Gây kích động nhân dân	07:00:00 28/01/2028	06:59:59 29/01/2028	miu.0602@icloud.com	Đối tượng 1
5	Kêu gọi lực lượng	07:00:00 27/01/2028	06:59:59 28/01/2028	miu.0602@icloud.com	Đối tượng 1

Hình 4.19. Điều tra dữ liệu lịch

- Tìm kiếm và phân tích dữ liệu ảnh và video trên thiết bị:



Thông tin ảnh

ExifTool Version Number : 12.87
 File Name : IMG_20230701_121750.jpg
 Directory : C:\Users\hacon\Desktop\image
 File Size : 5.6 MB
 File Modification Date/Time : 2023:07:01 12:17:53+07:00
 File Access Date/Time : 2024-09-19 21:07:00+07:00
 File Creation Date/Time : 2024-09-19 21:06:08+07:00
 File Permissions : -rw-rw-rw-
 File Type : JPEG
 File Type Extension : .jpg
 MIME Type : image/jpeg
 Exif Byte Order : Big-endian (Motorola, MM)
 Camera Model Name : Mi 9T
 Orientation : Rotate 90 CW
 Modify Date : 2023:07:01 12:17:53
 Y Cb Cr Positioning : Centered
 ISO : 112
 Exposure Program : Program AE
 F Number : 1.8
 Exposure Time : 1/2078
 Sensor type : rear
 AI Scene : 0
 Filter Id : 68048
 Hdr : off

Vị trí

20°48'18.2"N 106°46'43.1"E
 20.805058, 106.778650

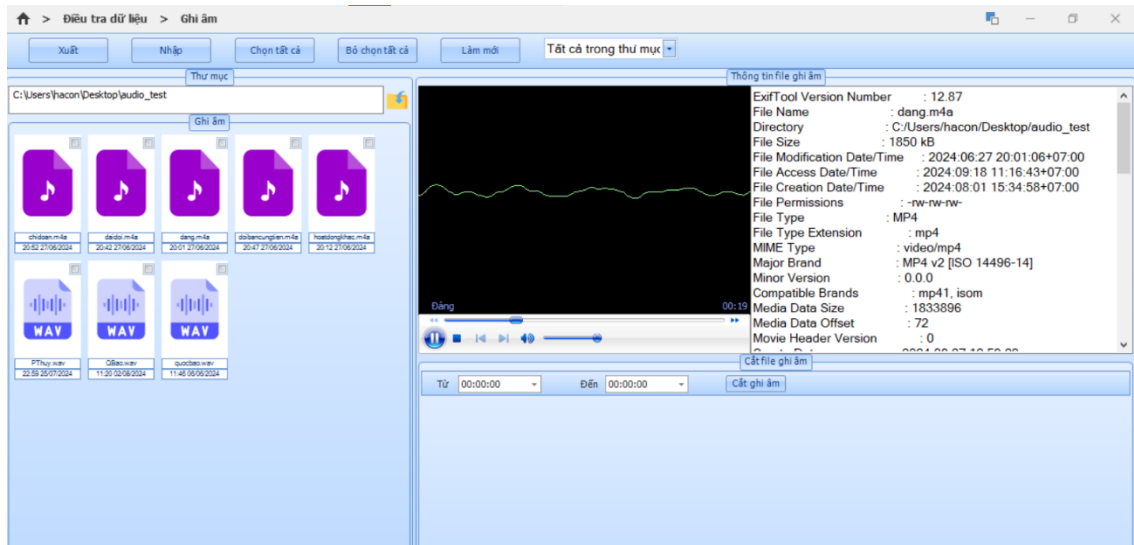
Restaurants
 Mác Thái 10
 Cầu Tân Vũ - Lạch Huyện
 DEEP C Hải Phòng IT
 Pantra Vina

KCN Đình Vũ, Đông Hải 2, Hải An, Hai Phong
 RQ4H+2FC Hải An, Hai Phong

Map data ©2024 Global Terms Privacy 100 m

Hình 4.20. Điều tra dữ liệu hình ảnh và video

- Tìm kiếm và phân tích dữ liệu âm thanh trên thiết bị:



Hình 4.21. Điều tra dữ liệu âm thanh

- Tìm kiếm và phân tích thông tin ứng dụng trên thiết bị:

The screenshot shows a table titled "Danh sách ứng dụng" (Application List) with the following columns: STT, Tên ứng dụng, Phiên bản, and Gói. The table contains 9 rows of data:

STT	Tên ứng dụng	Phiên bản	Gói
1	Quản lý phân động	CFBundleVersion	CFBundleIdentifier
2	Hội nhà nước Dega	8.6.5.0	com.campmobile.snow
3	Những người đứng đầu tổ chức Fogo	3.8.30.0	com.linecorp.Foodie
4	Quản lý kinh phí được tài trợ	41	com.music.pro.MusicPro
5	Messenger	350261955	com.facebook.Messenger
6	Zalo	432	vn.com.vng.zingalo
7	Gacha Club	2.0.0	com.lunime.gachaclub
8	YouTube	15.22.4	com.google.ios.youtube
9	Facebook	339817400	com.facebook.Facebook

Hình 4.22. Điều tra danh sách ứng dụng

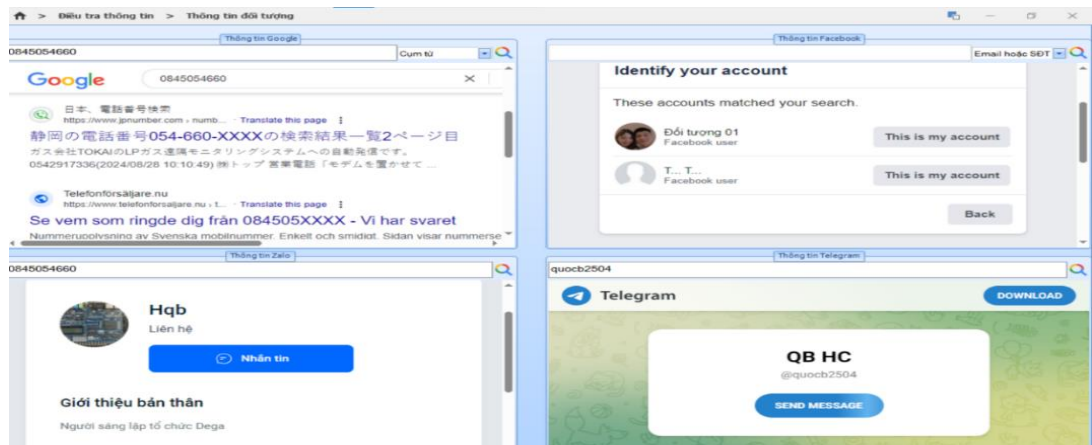
- Tìm kiếm và phân tích dữ liệu lịch sử duyệt web trên thiết bị:

The screenshot shows a table titled "Lịch sử truy cập" (Browsing History) with the following columns: STT, Thời gian, Tiêu đề, Đường dẫn, and Sao chép. The table contains 2 rows of data:

STT	Thời gian	Tiêu đề	Đường dẫn	Sao chép
1	11:22:31 04/07/2024	Cách tổ chức cuộc bạo loạn hiệu quả	https://www.google.com.vn/search?q=youtube&ie=UTF-8&oe=UTF-8&hl=vi-vn&client=...	Sao chép liên kết ▼
2	11:22:28 04/07/2024	Cách kêu gọi người dân theo tổ chức Dega	https://www.google.com.vn/ur?q=https://m.youtube.com/%3FH%3Dvi&sa=U&ved=2a...	Sao chép liên kết ▼

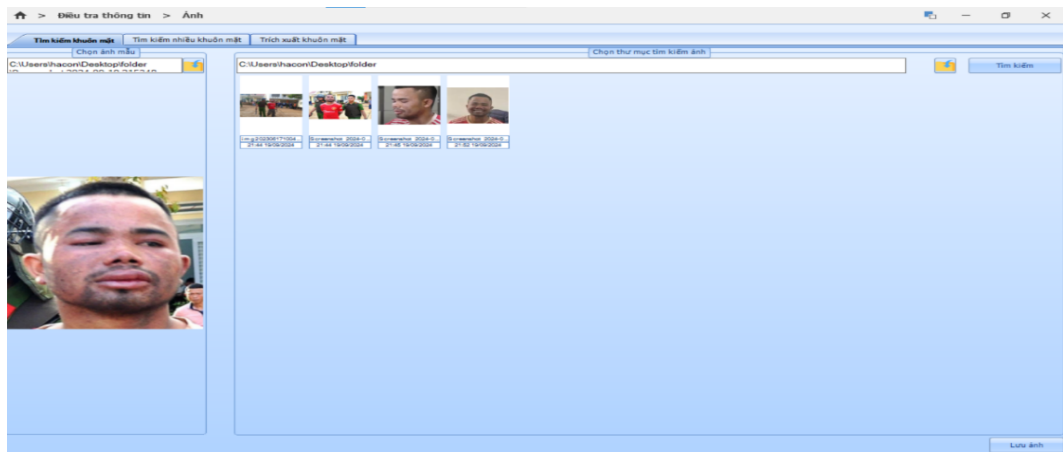
Hình 4.23. Điều tra dữ liệu duyệt web

- Tìm kiếm thông tin đối tượng trên thiết bị:



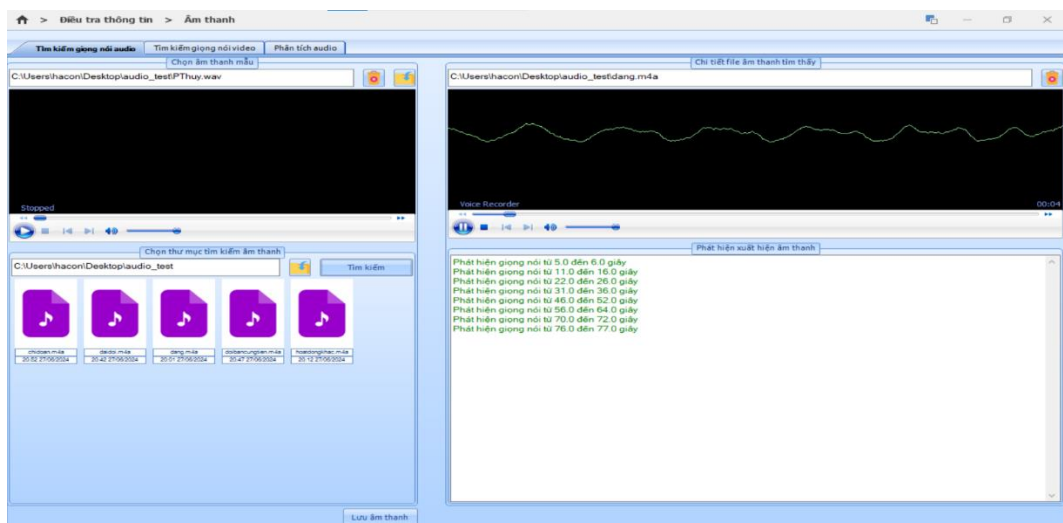
Hình 4.24. Tìm kiếm thông tin đối tượng

- Phân tích và tìm kiếm ảnh và video theo đối tượng trên thiết bị:



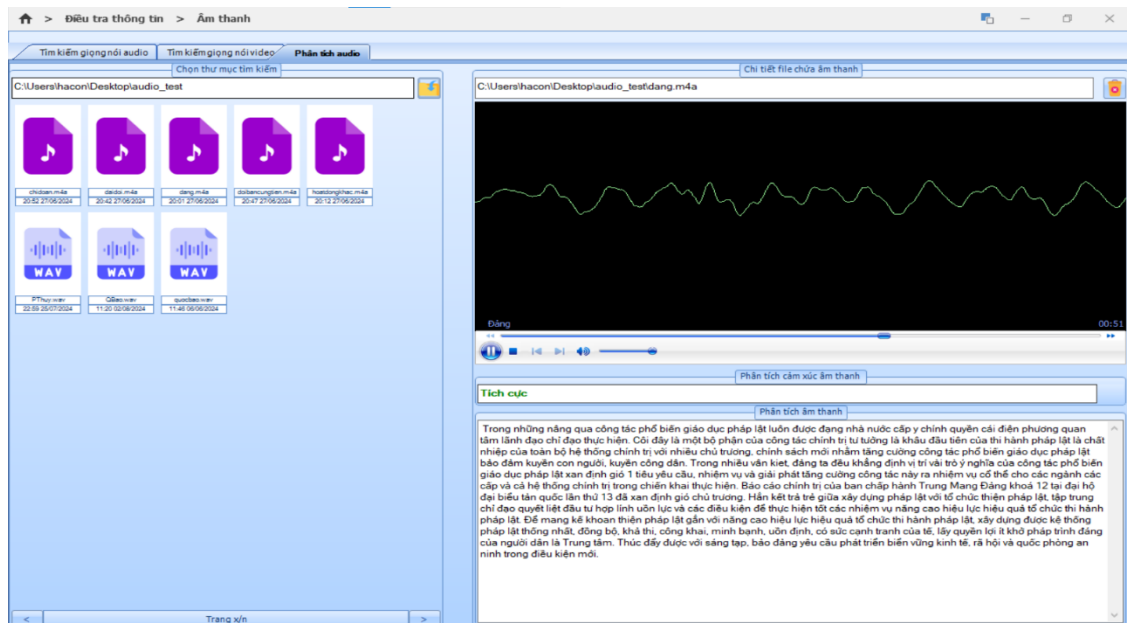
Hình 4.25. Tìm kiếm danh sách hình ảnh theo đối tượng

- Trích xuất tìm kiếm giọng nói trong danh sách tệp âm thanh:



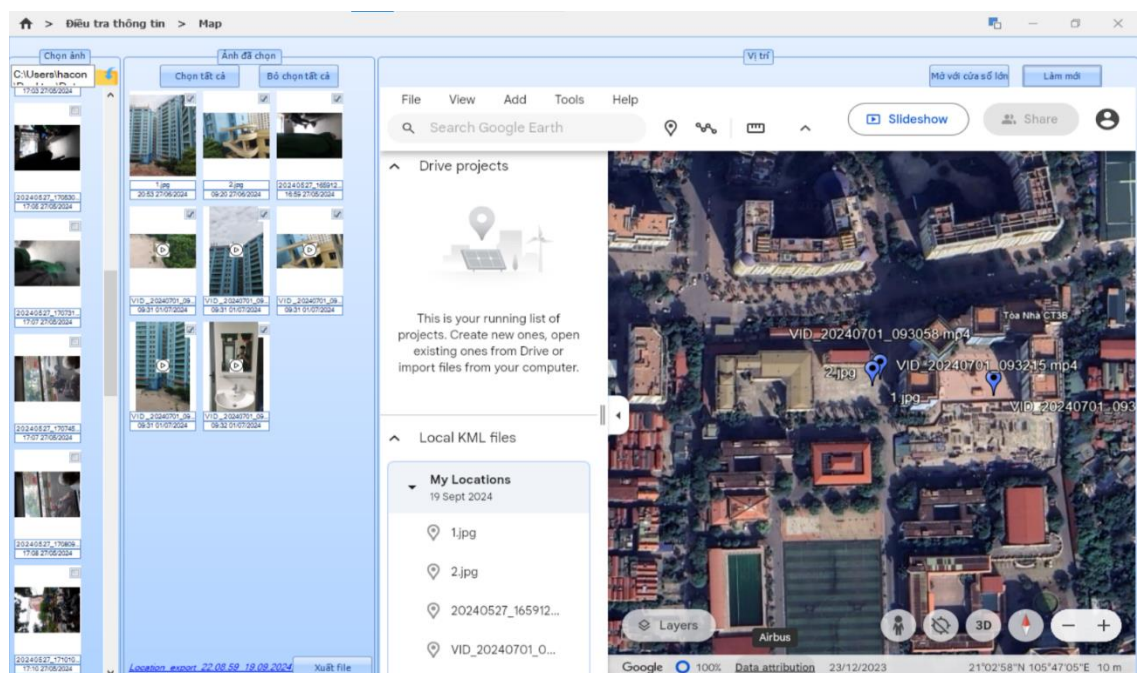
Hình 4.26. Tìm kiếm giọng nói của đối tượng

- Phân tích dữ liệu từ file âm thanh:



Hình 4.27. Phân tích file tài liệu

- Tìm kiếm và phân tích thông tin đối tượng từ dữ liệu vị trí của ảnh và video trên thiết bị:



Hình 4.28. Phân tích và điều tra dữ liệu vị trí

Bước 4: Tạo báo cáo điều tra: Người điều tra tạo báo cáo về kết quả điều tra dữ liệu trên thiết bị:

TỔ CHỨC ... <u>CƠ QUAN</u> ...	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM <u>Độc lập – Tự do – Hạnh phúc</u>					
Hà Nội, ngày 10 tháng 9 năm 2024						
BÁO CÁO KẾT QUẢ ĐIỀU TRA SỐ						
Trên thiết bị: iPhone 5s						
Người thực hiện điều tra: Hà Công Quốc Bảo						
Thời gian phiên điều tra: 10 giờ 10 phút, ngày 10 tháng 9 năm 2024						
Số serial thiết bị: c15bf3cd0766f2f153c398004ca0e2639b3d72ba						
Thư mục sao lưu: E:\Backup_IOS\Backup_export_10.09.2024						
Tệp dữ liệu sao lưu: E:\Backup_IOS\ c15bf3cd0766f2f153c398004ca0						
KẾT QUẢ THỰC HIỆN ĐIỀU TRA:						
1. Dữ liệu tin nhắn:						
STT	Loại tin nhắn	Người gửi	Người nhận	Nội dung	Thời gian	Sim
1	Nhận	Nguyễn Văn A (0987654321)	Thiết bị	Xin chào, dự án hôm nay tiến hành như thế nào rồi?	2023-11-20 10:30:00	1
2	Gửi	Thiết bị	Nguyễn Văn A (0987654321)	Tiến độ của vụ việc thế nào rồi?	2023-11-20 10:25:00	2

Hình 4.29. Báo cáo kết quả phiên điều tra

3. Kịch bản 3: Sử dụng kỹ nghệ xã hội thực hiện điều tra số trên thiết bị di động Android

3.1. Mô tả kịch bản

3.1.1. Kịch bản

Phát triển một ứng dụng điện thoại sử dụng kỹ nghệ xã hội để lừa dối người đã được xác định từ trước cài đặt ứng dụng lên thiết bị di động của họ. Khi người dùng mở ứng dụng, họ sẽ được yêu cầu thiết lập mật khẩu dưới dạng: PIN, hình vẽ hoặc mật khẩu ký tự. Mật khẩu này có thể trùng với mật khẩu màn hình khóa của thiết bị. Nhờ đó, khi thu giữ thiết bị, ta có thêm cơ sở để hỗ trợ việc bẻ khóa thiết bị, phục vụ cho điều tra số.

3.1.2. Các bước tiến hành

Bước 1: Dùng kỹ nghệ xã hội lừa người dùng cài đặt và sử dụng: Tận dụng yếu tố tâm lý và thiếu hiểu biết về an ninh mạng để đánh lừa người dùng cài đặt ứng dụng, từ đó thu thập mật khẩu.

Bước 2: Thu giữ và mở khóa thiết bị: Sau khi đã lừa người dùng cài đặt ứng dụng, có thể dự đoán được mật khẩu. Khi thiết bị bị thu giữ để tiến hành điều tra sử dụng thông tin thu được từ ứng dụng để hỗ trợ mở khóa thiết bị.

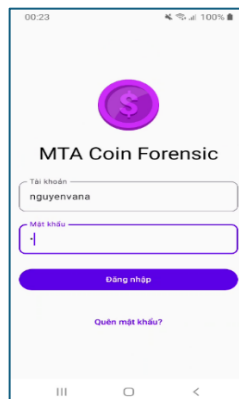
Bước 3. Sao lưu dữ liệu thiết bị: Dữ liệu trên thiết bị được sao lưu để phân tích và điều tra, phát hiện bằng chứng hoặc thông tin phục vụ điều tra.

Bước 4. Điều tra dữ liệu thiết bị: Thực hiện việc phân loại và phân tích toàn diện các dữ liệu đã thu thập để làm rõ hành vi củng cố bằng chứng hỗ trợ cho việc điều tra đối tượng.

Bước 5. Báo cáo dữ liệu thu được: Dữ liệu thu được sau khi phân tích sẽ được sử dụng để lập báo cáo chi tiết, làm căn cứ cho các hành động pháp lý.

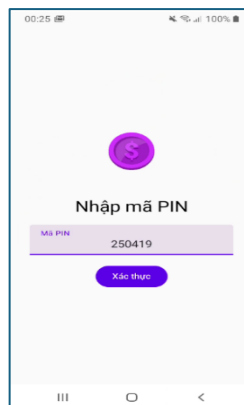
3.2. Thứ tự hành động

Bước 1: Xây dựng công cụ để dùng kỹ nghệ xã hội lừa đối tượng: Xây dựng một ứng dụng di động khai thác tiền ảo nhằm đánh lừa người dùng đăng ký và cài đặt:



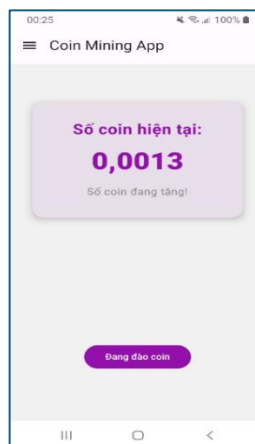
Hình 4.30. Giao diện đăng nhập của ứng dụng

- Đối tượng sau khi đăng nhập thành công tài khoản thì ứng dụng yêu cầu nhập mã pin của ứng dụng. Thông thường đối tượng thường chủ quan đăng ký mật khẩu mã PIN của ứng dụng trùng với mã PIN của thiết bị di động. Lợi dụng yếu tố chủ quan này để trình sát trước mật khẩu mã PIN của đối tượng:



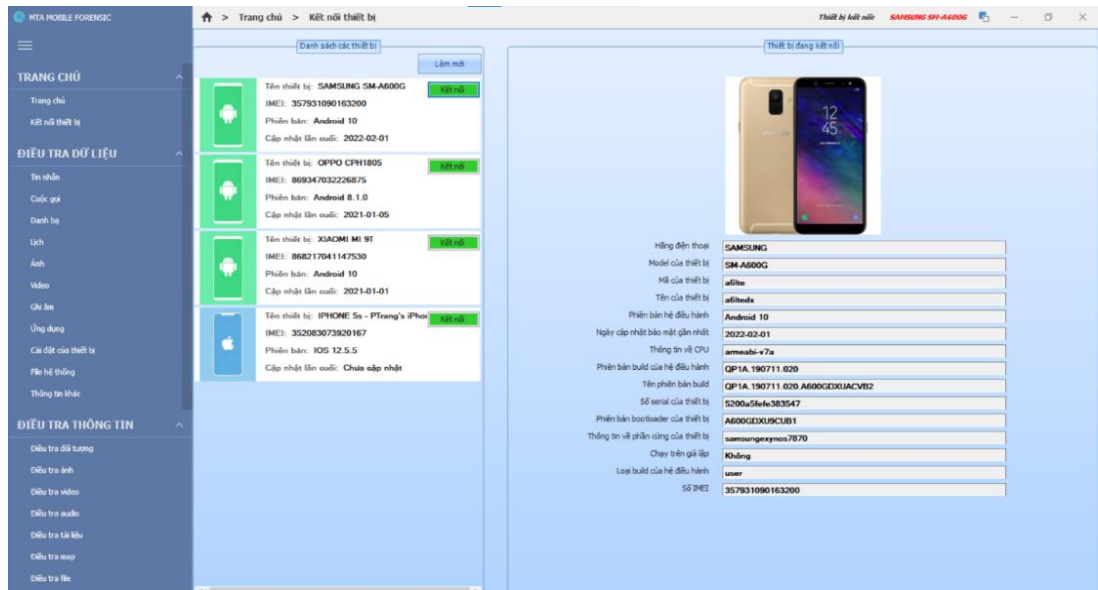
Hình 4.31. Giao diện nhập mã PIN ứng dụng

- Khi đối tượng đăng nhập và nhập mã PIN thành công, gửi mã PIN đối tượng vừa nhập về Server và chuyển giao diện về giao diện chính của ứng dụng:



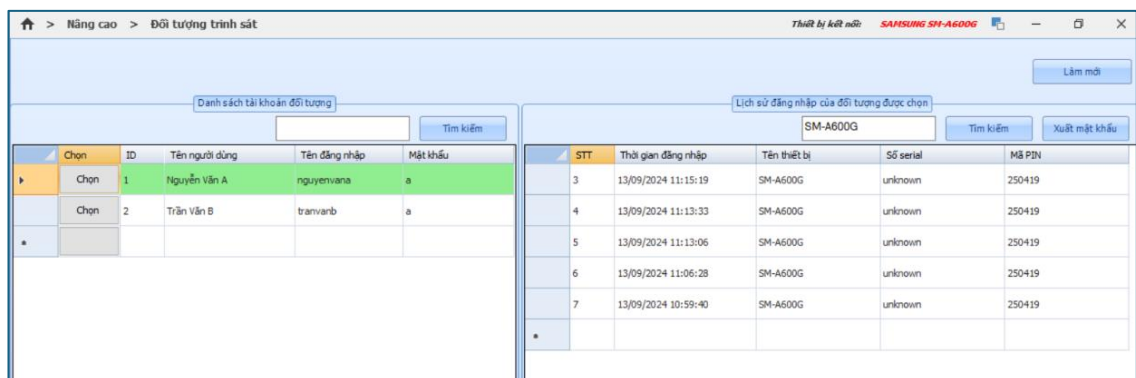
Hình 4.32. Giao diện chính của ứng dụng

Bước 2: Tiếp nhận và kết nối thiết bị: Trong trường hợp thu giữ được thiết bị của đối tượng nhưng đối tượng không cung cấp mật khẩu. Người điều tra tiếp nhận thiết bị và kết nối thiết bị với công cụ điều tra số MTA Mobile Forensic.



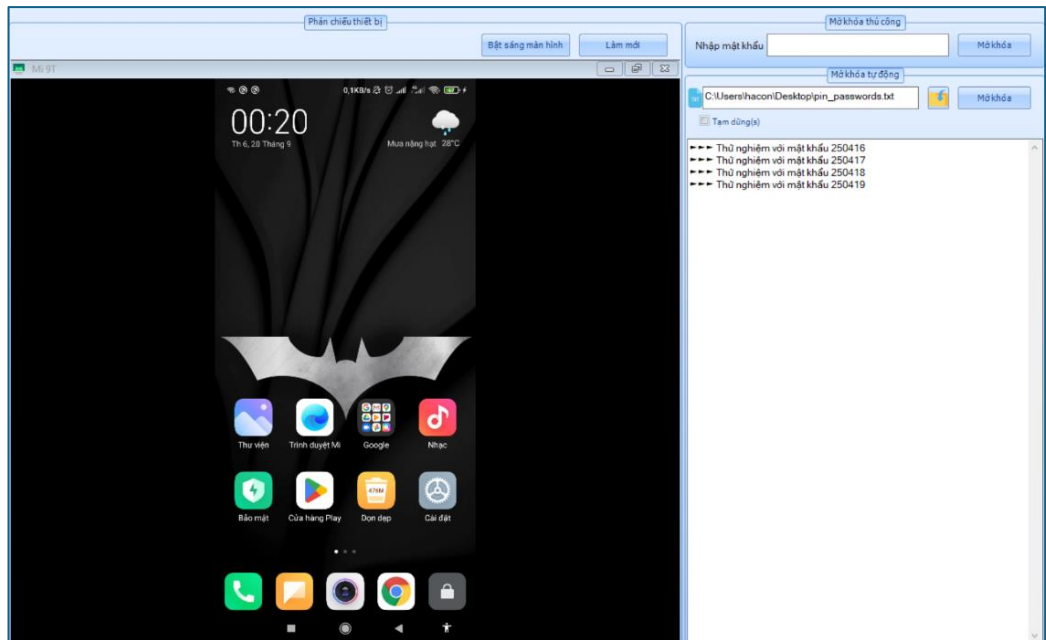
Hình 4.33. Kết nối thiết bị để điều tra

Bước 3: Tìm kiếm mật khẩu thiết bị trong danh sách đối tượng: Người điều tra chọn đối tượng đã có trên công cụ để tìm kiếm mã PIN mà đối tượng sử dụng trên thiết bị điều tra. Từ đó, người điều tra sẽ có căn cứ xây dựng danh sách mật khẩu để mở khóa được thiết bị:



Hình 4.34. Danh sách đối tượng trình sát

Bước 4: Thử và kiểm tra bằng danh sách mật khẩu có sẵn: Người điều tra xuất danh sách mã PIN đã có, sử dụng chứng năng mở khóa thiết bị để tiến hành mở khóa tự động bằng danh sách mật khẩu có sẵn:



Hình 4.35. Sử dụng chức năng mở khóa tự động để mở khóa thiết bị