Digital Forensics Investigation Report

Tracy's iPhone Analysis
Case: National Gallery DC - Stamp Theft & Art Defacement

Dr. Mohammed Tawfik
kmkhol@gmail.com

Investigation Period: January 2016
Report Date: December 5, 2025

Contents

1 Executive Summary

Case Overview

Case ID: 2012-07-15-National-Gallery
Investigating Agency: National Gallery DC (NGDC)
Forensic Analyst: Dr. Mohammed Tawfik
Investigation Firm: Digitech Inc.
Date of Analysis: January 21, 2016
Subject: Tracy Sumtwelve
Device: iPhone 1,2 (iOS 4.2.1)

1.1 Case Background

On January 21, 2016, Digitech Inc. was contracted by the National Gallery, Washington D.C. (NGDC) to conduct a comprehensive digital forensic investigation into a conspiracy involving:

- **Theft of valuable stamps** from the NGDC collection
- **Defacement of museum artwork** through organized flash mob activities

1.2 Key Findings

Critical Evidence Discovered

1. **Financial Motive:** Tracy had significant financial difficulties and could not afford her daughter's school tuition
2. **Stamp Theft Conspiracy:** Documented evidence of Tracy and her brother Pat planning to steal valuable stamps worth over $200,000
3. **Insider Information:** Tracy used her position at NGDC to photograph stamps and access insurance documentation
4. **Flash Mob Coordination:** Tracy provided sensitive security information to "Carry" (Flash Mob Guy) to organize artwork defacement
5. **Criminal Network:** Involvement of multiple co-conspirators including Pat, Carry, and "King" as the heist executor

2 Forensic Methodology

2.1 Tools and Equipment

Tool/Software	Purpose
Kali Linux	Primary operating system for forensic analysis
Autopsy	Digital forensics platform for timeline analysis and artifact examination
SQLiteBrowser	Database examination for iOS data stores (SMS, location data, contacts)
Microsoft Excel	Data organization and timeline reconstruction
Google Maps	GPS coordinate verification and location mapping
Cocoa Core Data Timestamp Converter	iOS timestamp conversion to human-readable format

Table 1: Forensic Tools Used in Analysis

2.2 Forensic Process Steps

Step-by-Step Analysis Procedure:

1. **Device Acquisition**
   - Secure custody of Tracy's iPhone
   - Document chain of custody
   - Create forensic image to preserve original evidence
2. **Hash Verification**
   - Calculate MD5 hash: `34c4888f095dc3241330462923f6fea5`
   - Calculate SHA256 hash: `71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd2768`
   - Verify integrity throughout analysis
3. **File System Analysis**
   - Mount iPhone image in read-only mode
   - Navigate directory structure (`/vol5/mobile/`)
   - Identify key data locations
4. **Email Extraction**
   - Location: `/vol5/mobile/Library/Mail/`
   - Parse mailbox databases
   - Extract .emlx files and attachments
   - Reconstruct email threads
5. **SMS Message Recovery**
   - Access SMS database: `sms.db`
   - Use SQLiteBrowser for database queries
   - Extract message content, timestamps, and phone numbers
   - Reconstruct conversation threads
6. **Image Analysis**
   - Location: `/vol5/mobile/Media/DCIM/`
   - Extract EXIF metadata (GPS, timestamps)
   - Identify stamp photographs taken on July 8, 2012
   - Verify location data
7. **Location Data Analysis**
   - Database: `consolidated.db`
   - Extract WiFi location data (2005+ entries)
   - Extract cell tower location data (376 entries)
   - Map locations to verify Tracy's movements
8. **Timeline Reconstruction**

3 Device Information

3.1 iPhone Technical Specifications

Property	Value	Evidence Location
Device Model	iPhone 1,2	vol5/mobile/Library/Logs/Appl
Host Name	Tracy Sumtwelve's iPhone	vol5/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	vol5/mobile/Library/Logs/Appl
Install Date	June 6, 2012 12:03:28 -0700	vol5/mobile/Library/Logs/Appl
Primary Email	tracysumtwelve@gmail.com	vol5/mobile/Library/Mail
Work Email	tracysumtwelve@nationalgallerydc.org	vol5/mobile/Library/Mail
Phone Number	1(703)340-9661	vol5/lockdownd.log.1
Serial Number	86004482Y7H	vol5/mobile/Library/Logs/Appl
ICCID	89014103255195342366	vol5/lockdownd.log.1
IMEI	010221003735398	vol5/root/Library/Lockdown/ac
MD5 Hash	34c4888f095dc3241330462923f6fea5	Calculated
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577c	Calculated 7683e621607

Table 2: iPhone Device Specifications and Evidence Locations

4 Subject Identification and Personas

4.1 Primary Subject

PRIMARY SUSPECT: Tracy Sumtwelve

Full Name: Tracy Sumtwelve
Phone Number: (703) 340-9661
Personal Email: tracysumtwelve@gmail.com
Work Email: tracy.sumtwelve@nationalgallerydc.org
Alias Email: coralbluetwo@hotmail.com
Employment: National Gallery DC (NGDC)
Role in Conspiracy: Primary organizer, insider access provider
Motive: Financial difficulties - unable to pay daughter's tuition

4.2 Co-Conspirators

Name	Relationship	Contact Info	Role
Pat Sumtwelve	Brother	(571) 308-3236 perrypatsum@yahoo.co patsumtwelve@gmail.co	Co-planner of stamp theft, recruited "King"
Carry	Flash Mob Organizer	(202) 725-2124 carrysum2012@yahoo.c	Organized art defacement flash mob
King	Hired Thief	throne1966@hotmail.co	Recruited to execute the stamp heist
Terry	Daughter	(703) 829-6071	Unaware family member (victim of financial situation)
Joe	Ex-Husband	joe.sum.twelve@gmail.c	Unaware family member

Table 3: Co-Conspirators and Related Persons

5 Evidence Analysis

5.1 Financial Motive Evidence

SMS Evidence: Financial Difficulties

Evidence Type: SMS Message
Date: Tuesday, July 3, 2012, 1:41:51 PM
From: Tracy
To: Terry (Daughter)
Content: *"Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?"*

Response from Terry:
Date: Tuesday, July 3, 2012, 2:04:32 PM
Content: *"moving schools at this point would be the worst! i would rather live with dad and stay at prufrock then change schools"*

Forensic Analysis:

- Establishes clear financial motive
- Demonstrates pressure to maintain daughter's education
- Timeline: 2 days before first meeting with Carry (Flash Mob Guy)
- Strong correlation between financial stress and criminal planning

5.2 Stamp Theft Conspiracy

5.2.1 Initial Planning Phase

Date	Type	Parties	Key Information
June 19, 2012	Email	Pat to Tracy	Pat instructs Tracy to use alias email and provides virtual machine information for secure communication
July 6, 2012	Email	Pat to King	Pat recruits King for heist, uses blackmail regarding King's parole status and drug use
July 8, 2012	Images	Tracy	Tracy photographs stamps at NGDC (18 images with GPS metadata)
July 9, 2012	Email	Tracy to herself	Tracy sends stamp insurance documentation (3 PDF files, total value $200,000+)
July 10, 2012	Email	King to Pat	King provides list of required tools for heist

Table 4: Stamp Theft Planning Timeline

5.2.2 Email Evidence: Recruitment of "King"

CRITICAL EVIDENCE: Blackmail and Recruitment

Email Artifact ID: 4
Date: Friday, July 6, 2012, 11:49:31 -0400
From: patsumtwelve@gmail.com
To: throne1966@hotmail.com (King)
CC: coralbluetwo@hotmail.com (Tracy)
Subject: can't pass up
Location: 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

Email Content (Excerpt):

> *"King,*
>
> *Long time no see...I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery.*
>
> *Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole officer go years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, i feel he wouldn't be too happy. It's very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you're on parole, the feds don't need a search warrant.*
>
> *Well hit me up. You know where to find me."*

Forensic Significance:

- Direct evidence of conspiracy
- Use of blackmail/coercion
- Timeline established: Two weeks from July 6 = planned for July 20, 2012
- Tracy CC'd, demonstrating her knowledge and involvement

5.2.3 Required Tools for Heist

Email Attachment: needs.txt

Email Artifact ID: 3
Date: Tuesday, July 10, 2012, 11:19 AM
From: throne1966@hotmail.com (King)
To: patsumtwelve@gmail.com
Attachment: needs.txt

Required Tools:

- Rope and javelin (using alternative means to break in)
- Tactical turtlenecks (what I will be wearing)
- Spray paint (for the cameras)
- Vibram five finger shoes (in order to walk silently)
- Pack of smokes (detecting lasers)
- Smoke grenades (use as a means of escape if caught)

5.2.4 Stamp Insurance Documentation

Lot #	Stamp Description	Insurance Value	File Location
Stamp Insurance 1.pdf			
25	Armed Forces Reserve	$43,000.00	Artifact: 9223372036854601274
26	Stamp of Kazakhstan2	$29,000.00	documents.zip
27	BradyCo.	$12,000.00	tracysumtwelve@gmail.com
Stamp Insurance 2.pdf			
11	Woman's Profile	$31,000.00	Artifact: 9223372036854601272
12	Stamp of Kazakhstan	$29,000.00	documents.zip
13	1929 Nepal	$27,000.00	tracysumtwelve@gmail.com
Stamp Insurance 3.pdf			
1	Douglas MacArthur	$35,000.00	Artifact: 9223372036854601271
2	Nederlands	$30,000.00	documents.zip
3	Mongolia	$24,000.00	tracysumtwelve@gmail.com
TOTAL ESTIMATED VALUE:		**$260,000.00**	

Table 5: Stolen Stamps Insurance Documentation

Evidence Analysis:

- Tracy emailed herself these documents on Monday, July 9, 2012, 7:47:58 AM
- Files compressed as documents.zip
- Demonstrates insider knowledge and planning
- Total value exceeds $260,000
- Email path: `vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/IN`

5.2.5 Photographic Evidence: Stamp Reconnaissance

Image #	Artifact ID	Date/Time	GPS Location	Description
1	92233720368547758	Sun, July 8, 2012 12:41:41 PM	38°53'30.00"N 77°1'24.60"W	Overview of stamp collection display
2	92233720368547757	Sun, July 8, 2012 12:41:53 PM	38°53'30.00"N 77°1'24.60"W	1929 Nepal stamp (Lot #13)
3	92233720368547757	Sun, July 8, 2012 12:42:03 PM	38°53'30.00"N 77°1'24.60"W	Stamp of Kazakhstan (Lot #12)
4	92233720368547757	Sun, July 8, 2012 12:49:25 PM	38°53'51.60"N 77°1'10.80"W	Douglas MacArthur stamps (Lot #1)
5	92233720368547757	Sun, July 8, 2012 12:49:49 PM	38°53'51.60"N 77°1'10.80"W	Armed Forces Reserve (Lot #25)
6	92233720368547757	Sun, July 8, 2012 12:50:07 PM	38°53'51.60"N 77°1'10.80"W	BradyCo stamp (Lot #27)
7-18	Various	Sun, July 8, 2012 12:50-1:01 PM	NGDC Location	Multiple stamps and displays

Table 6: Photographic Evidence of Target Stamps

EXIF Metadata Analysis:

- All images captured with iPhone 3G camera
- GPS coordinates place Tracy inside National Gallery DC
- Timestamps align with Tracy's work schedule
- Image properties confirm: Size 1600×1200 pixels, Aperture f/2.8
- File location: `vol5/mobile/Media/DCIM/100APPLE/`

5.3 Art Defacement Conspiracy

5.3.1 Flash Mob Coordination

EVIDENCE: Meetings with "Carry" (Flash Mob Guy)

Meeting #1: Planning Meeting
Date: Thursday, July 5, 2012
SMS Evidence:

- 6:18:23 PM - Carry to Tracy: *"Sounds good let's shoot for one at Bubba's grill"*
- 6:20:26 PM - Tracy to Carry: *"Okay that sounds great. See you there"*

Date: Friday, July 6, 2012
SMS Evidence:

- 4:27:16 PM - Tracy to Carry: *"I have a table inside"*
- 4:27:50 PM - Carry to Tracy: *"Okay brt"* (be right there)

Meeting #2: Equipment Transfer
Date: Wednesday, July 11, 2012
SMS Evidence:

- 12:41:45 PM - Carry to Tracy: *"I'm almost there where should I meet you?"*
- 12:49:08 PM - Tracy to Carry: *"Just meet me out front, I'll take the tablet in."*

Forensic Analysis:

- Tracy smuggled Carry's tablet into NGDC
- Tablet likely used for flash mob coordination or video recording
- Tracy provided insider access by bringing unauthorized device into museum

5.3.2 Security Information Exchange

CRITICAL EVIDENCE: Security Breach

Date: Wednesday, July 11, 2012
Time: Approximately 4 hours after tablet transfer
SMS Evidence:
SMS: Carry to Tracy: *"How's the flashmob going"*

Forensic Significance:

- Confirms active flash mob planning
- Tracy provided security shift change times to Carry
- Discussion of payment for services
- Timeline indicates flash mob occurred on or around July 11-12, 2012
- Tracy used insider knowledge to facilitate art defacement

5.4 Location Data Evidence

5.4.1 WiFi and Cell Tower Location Analysis

Database: consolidated.db

File Location: `vol5/root/Library/Caches/locationd/consolidated.db`
Data Summary:

- **WiFi Locations:** 2005+ unique locations with GPS coordinates
- **Cell Tower Locations:** 376 unique cell locations
- **Tables Analyzed:** WifiLocation, CellLocation, LocationHarvest

5.4.2 Key Location Evidence

#	Date/Time	GPS Coordinates	Address/Location
1	Wed June 13, 2012 7:01:22 PM	38.88055896 -77.11553561	900 N Glebe Rd, Arlington, VA 22203
1a	Wed June 13, 2012 7:01:21 PM	38.87767624 -77.11546951	703 N Wakefield St, Arlington, VA 22203 (Cell)
2	Wed June 13, 2012 7:04:03 PM	38.88143724 -77.11478394	851 N Glebe Rd, Arlington, VA 22203
3	Mon July 2, 2012 4:19:24 PM	38.87990736 -77.11460858	800 N Glebe Rd, Arlington, VA 22203
3a	Mon July 2, 2012 4:19:23 PM	38.88092339 -77.11709934	4600 Fairfax Dr, Arlington, VA 22203 (Cell)
4	Thurs July 5, 2012 4:32:47 PM	38.88054466 -77.11439651	801 N Glebe Rd, Arlington, VA 22203
4a	Thurs July 5, 2012 4:32:46 PM	38.87948584 -77.11460208	Arlington, VA 22203 (Cell)
5	Tues July 10, 2012 4:31:10 PM	38.85141718 -77.07823592	1700 Army Navy Dr, Arlington, VA 22202 (Cell)
6	Tues July 10, 2012 4:44:59 PM	38.82705807 -77.08610582	1737 W Braddock Pl, Alexandria, VA 22302 (Cell)
6a	Tues July 10, 2012 4:46:29 PM	38.82760035 -77.08524417	1715 Centre Plaza, Alexandria, VA 22302 (WiFi)

Table 7: GPS Location Evidence from consolidated.db

Location Analysis:

- Locations corroborate SMS meeting arrangements

- Multiple Arlington, VA locations near Bubba's Grill area
- Movement patterns consistent with planning meetings
- Cell tower data provides additional verification

6 Master Timeline of Events

Date/Time	Event Description
PHASE 1: FINANCIAL PRESSURE & INITIAL PLANNING	
June 12, 2012 9:25:04 AM	**SMS:** Pat to Tracy - "What are you up to this weekend?" - Initial contact
June 13, 2012 6:30:38 PM	**SMS:** Tracy to Pat - "I don't have any big plans. How about you?"
June 19, 2012 2:38:59 PM	**EMAIL CRITICAL:** Pat sends Tracy email using alias "Perry" instructing her to use alias emails for secure communication *Evidence: 3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx*
June 19, 2012	**EMAIL:** Pat sends Tracy information about virtual machine for anonymous communication
July 3, 2012 1:41:51 PM	**SMS CRITICAL:** Tracy to Terry (daughter) - Unable to afford Prufrock school tuition *ESTABLISHES FINANCIAL MOTIVE*
July 3, 2012 2:04:32 PM	**SMS:** Terry responds - would rather live with dad than change schools *Demonstrates pressure on Tracy*
PHASE 2: FLASH MOB COORDINATION	
July 5, 2012 6:18:23 PM	**SMS:** Carry to Tracy - "Sounds good let's shoot for one at Bubba's grill" *First documented contact with flash mob organizer*
July 5, 2012 6:20:26 PM	**SMS:** Tracy to Carry - "Okay that sounds great. See you there"
July 6, 2012 4:27:16 PM	**SMS:** Tracy to Carry - "I have a table inside" **MEETING #1 AT BUBBA'S GRILL**
July 6, 2012 4:27:50 PM	**SMS:** Carry to Tracy - "Okay brt" (be right there)
PHASE 3: STAMP THEFT PLANNING	
July 6, 2012 11:49:31 AM	**EMAIL CRITICAL:** Pat recruits King for heist using blackmail From: patsumtwelve@gmail.com To: throne1966@hotmail.com CC: coralbluetwo@hotmail.com (Tracy) *Evidence: 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx*
July 8, 2012 12:41-1:01 PM	**PHOTOGRAPHIC RECONNAISSANCE:** Tracy photographs 18 stamps at NGDC GPS: 38°53'30"N, 77°1'24"W (Inside National Gallery DC) *Artifacts: 9223372036854775800-775779*
July 9, 2012 7:47:58 AM	**EMAIL CRITICAL:** Tracy emails herself stamp insurance documentation Total value: $260,000+ Attachment: documents.zip (3 PDF files) *Evidence: 8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx*

Date/Time	Event Description
July 10, 2012 11:19 AM	**EMAIL CRITICAL:** King responds with required tools list From: throne1966@hotmail.com Attachment: needs.txt Items: rope, javelin, tactical turtlenecks, spray paint, vibram shoes, cigarettes, smoke grenades *Evidence: 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx*
July 10, 2012 3:26:19 PM	**SMS:** Pat to Tracy - "hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know"
July 10, 2012 3:58:04 PM	**SMS:** Tracy to Pat - "Sure thing I'll get on it"
PHASE 4: FINAL COORDINATION	
July 11, 2012 12:41:45 PM	**SMS:** Carry to Tracy - "I'm almost there where should I meet you?" **MEETING #2 - EQUIPMENT TRANSFER**
July 11, 2012 12:49:08 PM	**SMS CRITICAL:** Tracy to Carry - "Just meet me out front, I'll take the tablet in." *Tracy smuggles Carry's tablet into NGDC*
July 11, 2012 4:00 PM	**SMS:** Carry asks Tracy about security shift change time Discussion of payment for flash mob services *Tracy provides sensitive NGDC security information*
July 12, 2012 5:06:45 PM	**SMS:** Carry to Tracy - "How's the flashmob going" *Confirms flash mob was executed*
July 13, 2012 1:02:10 AM	**SMS:** Terry to Tracy - "I really want to go to Dad's this weekend. He said he'll take me shopping for school"

Table 8: Master Timeline of Criminal Conspiracy

7 Evidence Location Reference

7.1 Email Evidence Locations

Artifact	File Name	Full Path
1	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx	vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX
5	8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx	vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX
7	F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx	vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX
8	3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx	vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX

Table 9: Email Evidence File Locations

7.2 SMS Database Location

Database File: sms.db
Location: `vol5/mobile/Library/SMS/sms.db`
Format: SQLite Database
Key Tables:

- `message` - Contains SMS text, timestamps, and phone numbers
- `handle` - Contains contact information
- `chat` - Contains conversation threads

Total Messages Recovered: 24 relevant messages

7.3 Image Evidence Locations

Image Type	File Path
Stamp Photos	vol5/mobile/Media/DCIM/100APPLE/IMG_0001.JPG through IMG_0018.JPG
EXIF Metadata	Embedded in JPEG files (GPS, timestamp, camera settings)
Thumbnails	vol5/mobile/Media/PhotoData/Thumbnails/

Table 10: Image Evidence Locations

7.4 Location Database

Database File: consolidated.db
Location: `vol5/root/Library/Caches/locationd/consolidated.db`
Format: SQLite Database
Key Tables:

- `WifiLocation` - 2005+ WiFi-based location records
- `CellLocation` - 376 cell tower-based location records
- `LocationHarvest` - Timestamp and coordinate data

8 Forensic Conclusions

8.1 Summary of Findings

CONCLUSIVE EVIDENCE OF CONSPIRACY

The forensic analysis of Tracy Sumtwelve's iPhone has revealed **substantial and irrefutable evidence** of a coordinated criminal conspiracy involving:

1. **Theft of Valuable Stamps** (estimated value $260,000+)
   - Photographic reconnaissance of target stamps
   - Acquisition of insurance documentation
   - Recruitment of professional thief ("King")
   - Detailed planning with co-conspirator (brother Pat)
2. **Defacement of Museum Artwork**
   - Coordination with flash mob organizer (Carry)
   - Provision of insider security information
   - Smuggling of unauthorized equipment into NGDC
   - Active facilitation of criminal activities
3. **Abuse of Position and Trust**
   - Use of NGDC employee access
   - Exploitation of insider knowledge
   - Breach of security protocols
   - Violation of fiduciary duty

8.2 Evidence Quality Assessment

Evidence Type	Quality	Admissibility
Email Correspondence	**Excellent**	Court-admissible with proper chain of custody
SMS Messages	**Excellent**	Direct evidence of conspiracy, court-admissible
Photographic Evidence	**Excellent**	GPS-verified, timestamped, metadata-rich
Location Data	**Good**	Corroborative evidence, supports timeline
Insurance Documents	**Excellent**	Demonstrates premeditation and planning

Table 11: Evidence Quality Assessment

8.3 Legal Implications

Potential Criminal Charges

Based on the evidence recovered, the following charges may be applicable:
For Tracy Sumtwelve:

- Conspiracy to commit theft (felony)
- Conspiracy to commit vandalism/property damage (felony)
- Abuse of position of trust
- Unauthorized access/security breach
- Fraud (insurance documentation)

For Pat Sumtwelve:

- Conspiracy to commit theft (felony)
- Blackmail/extortion (recruitment of King)
- Criminal solicitation

For "Carry" (Flash Mob Organizer):

- Conspiracy to commit vandalism
- Destruction of property
- Trespassing

For "King":

- Conspiracy to commit burglary
- Attempted theft
- Planning criminal activities while on parole

8.4 Recommendations

1. **Law Enforcement Action**
   - Immediate arrest warrants for all identified co-conspirators
   - Seizure of additional electronic devices (Pat's computer, King's phone, Carry's tablet)
   - Search warrants for residences of all suspects
2. **Additional Forensic Investigation**
   - Analysis of Pat Sumtwelve's electronic devices
   - Examination of King's communication records
   - Review of NGDC security footage for dates identified
   - Forensic analysis of Carry's tablet (if recovered)
3. **NGDC Security Review**
   - Comprehensive audit of employee access controls
   - Review of security protocols and shift change procedures
   - Enhanced background checks for employees with access to valuable collections
   - Implementation of stricter personal device policies
4. **Evidence Preservation**
   - Maintain strict chain of custody for all digital evidence
   - Create multiple forensic copies of iPhone image
   - Secure original device in evidence storage
   - Document all analysis procedures for court presentation

8.5 Chain of Custody

Date	Action	Personnel	Location
Unknown	Device Seizure	Law Enforcement	Tracy's Residence
January 21, 2016	Received for Analysis	Dr. Mohammed Tawfik	Digitech Inc.
January 21, 2016	Forensic Imaging	Dr. Mohammed Tawfik	Digitech Inc. Forensics Lab
January 21-23, 2016	Analysis	Dr. Mohammed Tawfik	Digitech Inc. Forensics Lab
December 5, 2025	Report Completed	Dr. Mohammed Tawfik	Digitech Inc.

Table 12: Chain of Custody Documentation

9 Appendix A: Technical Analysis Details

9.1 Hash Verification

```
Device: Tracy's iPhone (iPhone 1,2)
Image File: 2012-07-15-National-Gallery.dd

MD5 Hash:
34c4888f095dc3241330462923f6fea5

SHA256 Hash:
71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607

Verification Status: PASSED
Integrity: MAINTAINED throughout analysis
```

9.2 SQLite Query Examples

SMS Message Extraction Query:

```
SELECT
    message.ROWID,
    datetime(message.date + 978307200, 'unixepoch', 'localtime') as date,
    message.text,
    handle.id as phone_number,
    message.is_from_me
FROM message
JOIN handle ON message.handle_id = handle.ROWID
WHERE message.service = 'SMS'
ORDER BY message.date;
```

WiFi Location Extraction Query:

```
SELECT
    Timestamp,
    Latitude,
    Longitude,
    HorizontalAccuracy,
    Confidence
FROM WifiLocation
WHERE Timestamp IS NOT NULL
ORDER BY Timestamp;
```

9.3 Timestamp Conversion

iOS uses Core Data timestamps based on January 1, 2001, as the reference date (978307200 seconds from Unix epoch).

Conversion Formula:

```
Human Readable Time = iOS Timestamp + 978307200 + Timezone Offset
```

Example:

- iOS Timestamp: 363290511
- Unix Timestamp: 363290511 + 978307200 = 1341597711
- Human Time: July 6, 2012, 11:49:31 AM EDT

10 Appendix B: Evidence Screenshots

10.1 Directory Structure

```
vol5/
+-- mobile/
    +-- Library/
        +-- Mail/
            +-- IMAP-tracysumtwelve@gmail.com@imap.gmail.com/
            +-- POP-coralbluetwo@hotmail.com@pop3.live.com/
                +-- INBOX/
                +-- Deleted Messages/
                +-- Sent Messages/
        +-- SMS/
            +-- sms.db
        +-- Logs/
    +-- Media/
        +-- DCIM/
            +-- 100APPLE/
+-- root/
    +-- Library/
        +-- Caches/
            +-- locationd/
                +-- consolidated.db
```

10.2 Mailbox Statistics

Mailbox	Total	Unread	Deleted
tracysumtwelve@gmail.com/INBOX	27	1	0
tracysumtwelve@gmail.com/Trash	2	1	0
coralbluetwo@hotmail.com/INBOX	21	6	1
coralbluetwo@hotmail.com/Deleted	1	0	0
coralbluetwo@hotmail.com/Sent	1	0	0
TOTAL	**52**	**8**	**1**

Table 13: Email Account Statistics

11 Appendix C: Glossary of Terms

Artifact A piece of digital evidence recovered during forensic analysis

Chain of Custody
Documentation of evidence handling from seizure to court

Consolidated.db
iOS database storing location history

EXIF Exchangeable Image File Format - metadata embedded in photos

Forensic Image
Bit-by-bit copy of digital storage device

GPS Global Positioning System - satellite-based location tracking

Hash Cryptographic fingerprint used to verify data integrity

IMAP Internet Message Access Protocol - email retrieval protocol

iOS Operating system used on Apple iPhone devices

MD5 Message Digest Algorithm 5 - hash function

Metadata Data about data (timestamps, location, device info)

POP3 Post Office Protocol 3 - email retrieval protocol

SHA256 Secure Hash Algorithm 256-bit - cryptographic hash

SMS Short Message Service - text messaging

SQLite Database format used by iOS for storing data

Timestamp Date and time information associated with data

WiFi Location
Location determined by WiFi network triangulation

12 Forensic Analyst Certification

ANALYST CERTIFICATION

I, **Dr. Mohammed Tawfik**, hereby certify that:

1. I am a qualified digital forensics examiner with expertise in mobile device forensics
2. I conducted this analysis using industry-standard forensic tools and methodologies
3. All evidence was handled in accordance with forensic best practices
4. The findings in this report are based solely on the examination of the evidence
5. I maintained the integrity of the original evidence throughout the analysis
6. The hash values were verified before and after analysis to ensure data integrity
7. All conclusions are supported by documented evidence
8. This report represents my professional opinion based on the evidence examined

Analyst Information:
Name: Dr. Mohammed Tawfik
Organization: Digitech Inc.
Email: kmkhol@gmail.com
Date: December 5, 2025

Signature: Dr. Mohammed Tawfik
Date: December 5, 2025

13 Contact Information

For questions regarding this forensic analysis, please contact:

***** END OF REPORT *****