Lab-Manual

Digital Forensics

CY-334L

AIR UNIVERSITY

DEPARTMENT OF
CYBER
SECURITY

**Prepared By: Ms.Memoona Sadaf**

**Instructor: Ms.Memoona Sadaf**

**Lab/Teaching Assistant: Muhammad Ahmad Ali Qureshi**

**Air University Islamabad**

AIR UNIVERSITY

Department of Cyber Security

Lab Schedule

| Week | Lab Topics |
|---|---|
| Week 9 | **Investigating and Preserving Evidence from Social Media Platforms** |

# Social Media Forensics Manual

**Table of Contents**

## 1. Introduction to Social Media Forensics

Social Media Forensics is a critical domain within digital forensics that deals with identifying, extracting, analyzing, and preserving evidence from social networking platforms. In the age of technology, a massive volume of human interaction takes place over platforms such as Facebook, Instagram, Twitter, WhatsApp, Snapchat, TikTok, and LinkedIn. These platforms store vast amounts of user-generated data, including messages, images, videos, metadata, and geolocation information.

Social media forensics helps law enforcement agencies, cybercrime investigators, and digital forensic professionals trace criminal activity, recover deleted data, monitor online threats, and maintain the integrity of digital evidence during investigations. It is frequently used in cases related to cyberbullying, online fraud, harassment, identity theft, terrorism, and missing persons.

### 2. Importance in Cyber Investigations

Social media forensics plays a key role in modern investigations for the following reasons:

- **Real-Time Communication Evidence**: Social media captures conversations as they happen. Posts, chat logs, likes, comments, and reactions can provide insight into a suspect's behavior.
- **User Activity Timeline**: Investigators can trace activities, sequence of events, and actions through timestamps, aiding in the reconstruction of criminal events.
- **Geolocation and Metadata**: Photos and videos uploaded often include metadata such as GPS coordinates, device type, and time, which can link suspects to a crime scene.
- **Digital Identity Tracing**: Each user interaction is linked to digital footprints such as IP addresses, MAC addresses, device identifiers, login locations, and network providers.
- **Behavioral Analysis**: Patterns in posting behavior, communication tone, and sudden changes in content can help develop psychological profiles.

---

### 3. Common Platforms Analyzed

Each platform presents unique types of evidence that can be analyzed during a forensic investigation:

| **Platform** | **Artifacts Collected** |
|---|---|
| **Facebook** | Messages, wall posts, group activity, reactions, friends, login logs |
| **Twitter** | Tweets, retweets, mentions, hashtags, DMs, followers |
| **Instagram** | Posts, reels, stories, comments, likes, messages, metadata |
| **WhatsApp** | Chat logs, call logs, voice notes, images, shared locations |
| **TikTok** | Video posts, likes, comments, music tags, GPS data |
| **LinkedIn** | Messages, profile updates, endorsements, activity logs |
| **Snapchat** | Snaps, chat messages, streaks, snap maps, memories archive |

---

### 4. Types of Evidence Collected

Investigators may encounter the following types of evidence during social media forensic analysis:

- **Screenshots** – Capturing visual data from posts, messages, and comments.
- **Metadata** – Information such as timestamps, IP addresses, device types, and geolocation embedded within digital files.
- **Chat logs and DMs** – Extracted from Facebook, Instagram, WhatsApp, Twitter, etc.

- **Archived or Deleted Content** - Tools can recover or uncover deleted posts and files.
- **Multimedia** - Images, videos, voice notes used as communication or evidence.
- **Geolocation Data** - Often stored within photo metadata or check-ins.
- **Social Connections** - Friend/follower lists, group affiliations.
- **Browser and Session Data** - Cookies, tokens, and login sessions stored in browsers.

## 5. Free & Popular Tools for Social Media Forensics

Numerous free tools are available to aid in social media forensic investigations. Here are some widely used ones:

| **Tool Name** | **Use Case** | **Free?** | **Website** |
|---|---|---|---|
| **SOCMINT** | Social media intelligence | Yes | Technique, not a tool |
| **Hunchly** | Web evidence capture and tracking | Yes | https://hunch.ly |
| **ExifTool** | Metadata extraction from images | Yes | https://exiftool.org |
| **Maltego** | Network and relationship mapping | Partial | https://maltego.com |
| **SpiderFoot** | Open-source footprinting tool | Yes | https://spiderfoot.net |
| **TweetBeaver** | Twitter data analysis | Yes | https://tweetbeaver.com |
| **Creepy** | Geolocation tracking | Yes | https://creepy.sourceforge.net |
| **OSINT Framework** | Collection of OSINT tools | Yes | https://osintframework.com |
| **Facebook Ad Library** | Viewing public ads | Yes | https://www.facebook.com/ads/library |

These tools allow forensic experts to extract public and private data (with legal permission), analyze metadata, map social networks, track geolocation, and archive content in a forensically sound manner.

## 6. Step-by-Step Investigation Process

### Step 1: Identify Platform and Suspect Data

Determine which platforms are relevant to the case. Gather basic account details, usernames, profile links, and screenshots for documentation.

### Step 2: Preserve the Evidence

- Create forensic copies using tools.
- Use screen recording or browser extensions to save volatile content.
- Record metadata, page source, and device logs.

### Step 3: Extract the Data

- Utilize APIs (Twitter API, Facebook Graph API) to extract structured data.
- Use Hunchly, ExifTool, TweetBeaver for image and text extraction.
- Access phone backups for platforms like WhatsApp (via tools like WhatsApp Viewer).

### Step 4: Analyze the Data

- Reconstruct timeline of events.
- Map communication chains.
- Identify behavioral red flags or suspicious links.
- Extract geolocation from media files.

### Step 5: Correlate with Other Evidence

- Match findings with call logs, GPS history, ISP data, device logs.
- Cross-reference with witness statements.

### Step 6: Document and Report

- Maintain logs of all activities, tools used, and outcomes.
- Prepare a professional forensic report with visuals, metadata, and citations.

## 7. Legal and Ethical Considerations

Social media forensic investigations must be conducted ethically and legally. Important factors include:

- **Chain of Custody**: Maintain detailed records to preserve the integrity of evidence.
- **Legal Authority**: Access to private data should be obtained via court orders.
- **Privacy Laws**: Follow data protection regulations (GDPR in Europe, PECA in Pakistan).
- **Non-Alteration of Data**: Any manipulation or forgery renders evidence inadmissible in court.
- **International Considerations**: Social media platforms may operate under different jurisdiction laws (e.g., US-based platforms with servers in Europe).

## 8. Sample Case Studies

### International Case

In January 2021, FBI investigators used posts and video evidence from TikTok and Instagram to identify and arrest multiple participants in the US Capitol Riots. Investigators relied on video metadata, timestamped selfies, and geotagged content posted online. The suspects were linked to specific areas within the Capitol through facial recognition and device identifiers.

### Pakistani Case

The FIA Cyber Crime Wing solved a high-profile blackmailing case in Lahore. The victim received threats via Facebook Messenger. Investigators extracted chat logs, traced login IP addresses, and obtained device logs from the suspect's internet provider. The suspect was located in Rawalpindi, and evidence was successfully presented in court.

---

## 9. Best Practices for Students

- **Practice with Virtual Labs**: Set up VMs to simulate real investigations.
- **Learn Tool Usage**: Start with Hunchly, ExifTool, and SpiderFoot.
- **Create a Checklist**: Include steps from identification to report writing.
- **Document Everything**: Keep logs of tools used, commands run, findings.
- **Stay Ethical**: Never access private content without permission.
- **Keep Updated**: APIs and platform policies change frequently.

---

## 10. References & Resources

- PECA Act 2016: https://na.gov.pk/uploads/documents/1470910659_707.pdf
- FIA Cyber Crime Wing: https://www.nr3c.gov.pk/
- "Digital Evidence and Computer Crime" by Eoghan Casey
- Hunchly Blog: https://www.hunch.ly/blog/
- OSINT Framework: https://osintframework.com
- ExifTool Documentation: https://exiftool.org
- TweetBeaver: https://tweetbeaver.com
- Creepy: https://creepy.sourceforge.net
- Maltego Community Edition: https://maltego.com

---