📘 STANDARD OPERATING PROCEDURE

Digital Evidence Collection Using Video Evidence Collector

SOP Number: DEV-001

Effective Date: January 15, 2024

Review Date: July 15, 2024

Authority: [Agency Head]

Distribution: All Investigative Personnel

---

1. PURPOSE

This SOP establishes standardized procedures for the collection, preservation, and documentation of digital video evidence from social media and online platforms using the Video Evidence Collector tool.

2. SCOPE

This procedure applies to all personnel authorized to collect digital evidence in the course of official investigations.

3. DEFINITIONS

- **Digital Evidence**: Electronic data from online platforms
- **Chain of Custody**: Documentation of evidence handling
- **Hash Value**: Digital fingerprint verifying file integrity
- **Evidence Package**: Complete collection including video, metadata, and documentation

4. RESPONSIBILITIES

4.1 Investigators

- Follow this SOP for all digital evidence collection
- Maintain chain of custody
- Document legal authority
- Secure evidence properly

4.2 Supervisors

- Ensure compliance with SOP
- Review evidence logs

- Approve sensitive collections
- Maintain training records

4.3 IT Support

- Maintain evidence collection tools
- Provide technical support
- Ensure secure storage
- Update software as needed

5. EQUIPMENT & SOFTWARE

5.1 Required Components

- Video Evidence Collector (VideoDownloader.exe)
- yt-dlp.exe (download engine)
- ffmpeg.exe (video processor)
- Windows 10/11 computer
- Secure storage device

5.2 System Requirements

- 8GB RAM minimum
- 100GB available storage
- Internet connection
- Administrator access

6. PROCEDURES

6.1 PRE-COLLECTION PHASE

Step 1: Legal Authority Verification

```
1.1 Confirm legal basis for collection:
    - Search warrant
    - Consent
    - Public domain
    - Exigent circumstances

1.2 Document authority in case file

1.3 If private content, obtain:
    - Specific warrant language
    - Written consent
    - Supervisor approval
```

Step 2: System Preparation

```
2.1 Verify tool installation:
    - Check all three files present
    - Confirm ffmpeg.exe installed
    - Test with public content

2.2 Create case folder:
    - C:\Cases\[CaseNumber]\
    - Set appropriate permissions

2.3 Open evidence log spreadsheet
```

6.2 COLLECTION PHASE

Step 3: Evidence Collection

```
3.1 Launch Video Evidence Collector

3.2 Configure settings:
    - Enable screenshot capture
    - Enable hash generation
    - Enable evidence report
    - Set output to case folder

3.3 For each piece of evidence:
    a. Copy URL from browser
    b. Paste into tool
    c. Verify platform detection
    d. Select appropriate quality
    e. Click Download
    f. Monitor progress
    g. Verify completion
```

Step 4: Private Content Collection

```
4.1 For browser cookie method:
    a. Log into platform via Chrome
    b. Enable "Use browser cookies"
    c. Proceed with download

4.2 For credential method:
    a. Enter authorized credentials
    b. Save encrypted
    c. Proceed with download

4.3 Document method used
```

6.3 POST-COLLECTION PHASE

Step 5: Evidence Verification

```
5.1 Open evidence folder

5.2 Verify contents:
    - Video file present
    - Evidence report generated
    - Screenshot captured (if available)
    - Metadata file saved

5.3 Review evidence report:
    - Confirm SHA256 hash
    - Check timestamps
    - Verify collector info
```

Step 6: Documentation

```
6.1 Update evidence log with:
    - Entry number
    - Collection date/time
    - Platform and URL
    - Evidence folder name
    - SHA256 hash
    - Legal authority

6.2 Complete chain of custody form

6.3 Add notes about collection
```

Step 7: Evidence Preservation

```
7.1 Create backup copy:
    a. Copy entire evidence folder
    b. To secure backup location
    c. Verify hash matches

7.2 Apply write protection:
    a. Right-click folder
    b. Properties > Read-only

7.3 Update backup log
```

6.4 QUALITY CONTROL

Step 8: Supervisor Review

```
8.1 Supervisor reviews:
    - Evidence log entries
    - Legal authority documentation
    - Evidence reports
    - Chain of custody

8.2 Supervisor signs off

8.3 File in case management system
```

7. SPECIAL SITUATIONS

7.1 Deleted Content

- Screenshot "Content Unavailable" message
- Document deletion in report
- Consider preservation letters

7.2 Multiple Videos

- Use queue feature for efficiency
- Maintain separate logs
- Group by suspect/platform

7.3 Emergency Collections

- Document exigent circumstances
- Collect first, document immediately
- Notify supervisor ASAP

7.4 Technical Failures

- Screenshot error messages
- Try alternative methods
- Contact IT support
- Document in case file

8. LEGAL CONSIDERATIONS

8.1 Warrant Limitations

- Stay within scope
- Don't exceed date range
- Respect privileged content
- Stop if unsure

8.2 Privacy Protection

- Minimize collateral collection
- Redact unrelated information
- Follow data retention policies
- Secure all evidence

8.3 Cross-Border Issues

- Check content origin
- Consider international law
- Consult legal counsel
- Document thoroughly

9. SECURITY REQUIREMENTS

9.1 Access Control

- Evidence folders restricted
- Password protect archives
- Log all access
- Regular audits

9.2 Data Handling

- No personal devices
- Encrypted storage only
- Secure disposal
- Clean workspace

9.3 Credential Management

- Never share passwords

- Change regularly
- Use official accounts only
- Report compromises

10. TRAINING REQUIREMENTS

10.1 Initial Training

- Complete video training
- Practice collection
- Pass competency test
- Supervisor sign-off

10.2 Ongoing Training

- Annual refresher
- Platform updates
- Legal updates
- New features

11. RECORD RETENTION

- Evidence files: Per case disposition
- Collection logs: 7 years
- Training records: 3 years
- SOP acknowledgments: 3 years

12. FORMS & ATTACHMENTS

- Appendix A: Evidence Log Template
- Appendix B: Chain of Custody Form
- Appendix C: Legal Authority Checklist
- Appendix D: Quick Reference Card

13. REVISION HISTORY

Version	Date	Changes	Approved By
1.0	01/15/24	Initial release	[Name]

ACKNOWLEDGMENT

I acknowledge that I have read, understood, and will comply with this Standard Operating Procedure.

Name: ______________________

Badge #: ____________________

Date: ______________________

Signature: __________________

This SOP is law enforcement sensitive. Do not distribute outside authorized personnel.