



COURT TESTIMONY GUIDE - DIGITAL EVIDENCE



PURPOSE

Prepare investigators to provide clear, credible testimony about digital evidence collected using the Video Evidence Collector tool.



PRE-TESTIMONY PREPARATION

Review Your Evidence Package

- ☐ Original evidence report
- ☐ SHA256 hash values
- ☐ Collection timestamps
- ☐ Chain of custody forms
- ☐ Your investigation notes
- ☐ Legal authority documents

Key Facts to Memorize

1. **Exact collection date and time**
2. **SHA256 hash of the video**
3. **Platform where content was found**
4. **Legal authority used**
5. **Any errors or issues encountered**

Practice Explaining Technical Concepts

- What is a hash value? *"A digital fingerprint unique to that exact file"*
 - What is metadata? *"Hidden information about when and how the file was created"*
 - What is chain of custody? *"Documentation showing who handled evidence and when"*
-



FOUNDATION QUESTIONS & ANSWERS

Q1: "How did you collect this video evidence?"

A: "I used a forensic tool called Video Evidence Collector. I entered the URL of the video, and the tool downloaded it while creating documentation including a screenshot, metadata, and an evidence report with a hash value for verification."

Q2: "Is this the same video that was online?"

A: "Yes. The tool downloads an exact copy. I can verify this through the SHA256 hash value, which is like a digital fingerprint. Any change to the file would produce a completely different hash."

Q3: "How do you know this video hasn't been altered?"

A: "I generated a SHA256 hash immediately upon collection. This hash is documented in my evidence report dated [date]. I can recalculate the hash today and it will match exactly, proving no alterations."

Q4: "What legal authority did you have?"

A: "I collected this evidence pursuant to [warrant/consent/public domain]. The specific authority is documented in my report and the case file."

Q5: "Could someone else have posted this?"

A: "I collected this from the defendant's verified account, which showed [profile details]. The URL I documented leads directly to their profile. However, I cannot definitively state who had access to post on the account."

DEMONSTRATIVE EVIDENCE

What to Bring to Court

1. **Printed evidence report** (highlighted key sections)
2. **Screenshot printouts** (if allowed)
3. **Chain of custody forms**
4. **Hash verification demonstration** (if requested)

Live Demonstration Checklist

If asked to demonstrate:

- ☐ Bring agency laptop with tool installed
 - ☐ Test courtroom display connectivity
 - ☐ Have backup plan (screenshots of process)
 - ☐ Practice with prosecutor beforehand
-

COMMON DEFENSE CHALLENGES

"The timestamp could be wrong"

Response: "The timestamp comes from multiple sources - my computer's system clock, the tool's evidence report, and the platform's metadata. All three align and my computer's time is regularly synchronized."

"Anyone could fake this"

Response: "The combination of the hash value, detailed metadata, and chain of custody documentation makes fabrication extremely difficult. Additionally, the defense can independently verify the content."

"You're not a computer expert"






Response: "I'm trained in digital evidence collection. I follow established procedures and use validated tools. The technical aspects like hash calculation are performed automatically by the tool."

"The tool could have errors"






Response: "The tool uses yt-dlp, which is open-source and widely validated. It downloads exactly what the platform provides. The hash verification confirms the integrity."

TESTIMONY BEST PRACTICES

DO:

-  Speak clearly and avoid jargon
-  Refer to your report for exact details
-  Admit if you don't know something
-  Explain technical concepts simply
-  Maintain professional demeanor

DON'T:

-  Guess or speculate
 -  Argue with attorneys
 -  Volunteer extra information
 -  Use technical terms without explaining
 -  State opinions beyond your expertise
-

TECHNICAL EXPLANATIONS FOR JURY

"What is a URL?"

"It's the web address you type or copy to visit a specific page - like a street address for the internet."

"What is downloading?"

"Making a copy of something from the internet onto your computer, like making a photocopy of a document."

"What is metadata?"

"Information about the file that's usually hidden - like the back of a photograph that shows when and where it was taken."

"What is a hash?"

"A unique code calculated from the file. If even one pixel changes, the entire code changes - like a tamper-evident seal."

"What is a screenshot?"

"A picture of exactly what appeared on my screen at that moment - like taking a photograph of a TV show."

SAMPLE DIRECT EXAMINATION

Prosecutor: "Detective, what is Exhibit 5?" **You:** "This is a video I downloaded from the defendant's Facebook page on [date] at [time]."

P: "How did you collect it?" **You:** "Using our digital evidence tool, I copied the URL and downloaded the video. The tool automatically created an evidence package."

P: "What is in the evidence package?" **You:** "The video file, a screenshot of the Facebook page, metadata about the video, and a detailed evidence report."

P: "Is Exhibit 5 an accurate copy?" **You:** "Yes. The SHA256 hash I generated then matches the hash today, confirming it's identical."

SAMPLE CROSS-EXAMINATION

Defense: "You don't know who posted this, do you?" **You:** "I know it was posted to the defendant's account. I cannot say who had access to that account."

D: "This could have been edited, correct?" **You:** "No. Any edit would change the hash value. The hash from collection matches today's hash."

D: "You just trust this tool?" **You:** "I follow established procedures. The tool is regularly validated and the hash verification provides independent confirmation."



POST-TESTIMONY NOTES

After testifying:

1. Document any unexpected questions
 2. Note any tool issues mentioned
 3. Update training based on experience
 4. Debrief with prosecutor
 5. File testimony notes with case
-



EMERGENCY RESPONSES

If you don't know: "I don't have that information available."

If confused: "Could you please rephrase the question?"

If technical issue: "I can explain that in simpler terms..."

If challenged on qualifications: "I've completed [X] hours of digital evidence training and have collected evidence in [X] cases."



RESOURCES

Technical Support During Trial:

- IT On-Call: _____
- Digital Forensics: _____
- Tool Expert: _____

Legal Support:

- Prosecutor: _____
 - Agency Counsel: _____
-

Remember: Your job is to present facts about what you did and what you found. Stay within your expertise and let the evidence speak for itself.

Last Updated: January 2024

Version: 1.0