Montana Department of Justice

Sexual Assault Kit Initiative

Course “Digital Evidence Collection”

Intro

Slide 2: Welcome to the course Digital Evidence Collection.

Slide 3: Content Warning: We will be talking about sexual violence which may trigger personal feelings. Please remember to take care of yourself and do what you need to help yourself.

Slide 4: Disclaimer: This project was supported by Grant No. 2017-AK-BX-0022 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice."

Slide 5: In this course, you will learn about the different types of technology and social media platforms and how to identify and collect digital evidence.

Slide 6: Digital evidence is information that is stored on, received, or transmitted in a digital format by an electronic device, such as a smart phone, step tracker (or Fitbit), and computers, that can be used in court to help prove a sexual assault occurred. It's reasonable to expect that, going forward, just about every investigation will include evidence collected from some sort of digital device. Examples of such evidence can include:

- When a person sends text messages that contain threats
- When a person creates harassing posts on social media
- When someone uses technology to stalk a victim, there may be evidence in the form of GPS tracking data, video footage, or spyware purchases
- Video(s) or photo(s) of the criminal act
- Planning or preparation of criminal activity
- Other victims

Slide 7: Menu

- **Technology**
- **Social Media**

Technology

Slide 8: What types of devices should you consider as possible evidence? Bear in mind the various ways people use technological devices and the various types of information they may contain. Anything with an on and off switch is a potential source of evidence, but particularly the following:

- Smart Phones

- Smart watches
- iPods and other portable players
- iPads and other tablets
- Computers
- Fitbits and other step trackers
- Cameras and other recording devices
- Storage devices, such as thumb drives, SD cards, external hard drives, or CDs and DVDs.

Slide 9: How do you identify evidence from a device? If you identify a technological device as evidence, you should also identify the type of evidence it may contain, such as:

- Images or videos of the act itself
- Dates and times embedded in the images or videos
- Data to corroborate a survivor's statement
- Location services
- Search history
- Conversation between survivor and suspect
- Admissions of a crime by suspect
- Timeline of survivor and/or suspect
- Heart rates
- Placing a suspect or survivor at the crime scene
- Apps and programs
- Other information

Slide 10: Also understand that technology may have played a role in facilitating the crime through

- the suspect threatening to destroy the survivor's technology
- communication with the survivor
- exploitation or threatening the survivor and/or survivor's family, friends, others

Slide 11: So, how should you collect evidence?

1) First and foremost, if the device is on, observe any information on the display, which is considered plain view and may be excluded from the search warrant requirement.
2) Next, place the device into a mode that will not transmit data, such as airplane mode, disabling the Wi-Fi, powering down the device, or even removing the battery, if easily accessible, to keep evidence from being destroyed remotely.
3) Do not try to guess the password. Entering wrong passwords might encrypt the device more with each try.
4) Now, provide the owner with a property receipt that identifies the device. Proper identification should include:
    - Make and model of the device
    - Color
    - Serial number

- Any specific description of the device, including identifying characteristics

5) If you are unsure about the use of a certain device, don't hesitate to google it. Instructions can be found for every function and every device.

Slide 12: Once the device is properly collected, secured, and does not transmit data, you will need to **store it correctly**.

1) Place the device into a container, such as a manila envelope or Ziploc bag.
2) Ensure the device is properly packaged and buffered to ensure it will not get damaged.
3) Seal the container with evidence tape, initial the evidence tape with your identifying information, date, case number, description of the evidence, and the property owner's name.
4) Attach an evidence tag to the storage container.
5) Place the device into a proper evidence receptacle.
6) If there is any risk that the device may transmit or be compromised by outside sources, place it in a Faraday bag to secure it from transmissions or wiping. A Faraday bag is a pouch with a layer of foam-padded nylon and two layers of material specifically designed to shield against radio frequencies and connectivity to cell towers or wi-fi access points.

Slide 13: Many devices can be connected to the internet through mobile data and wireless carriers, such as Verizon, AT&T, T-Mobile, Sprint, or other local carriers. You can take advantage of these connections by collecting the following information:

- Subscriber information
- Physical billing address
- Type of devices
- Call logs, such as incoming, outgoing, durations
- Text message logs
- Some text messaging content with limited retention
- Connectivity records, such as tower location
- Photo or image storage

Slide 14: To learn about what information can be obtained from a wireless company and what legal process must be followed to obtain such information, you should:

- Access the SEARCH website, which provides important information on how to deal with technology-related issues. SEARCH provides access to law enforcement reference guides to help navigate wireless companies legal process requirements as well as information obtained. The website is www.search.org.
- Use Montana's criminal justice information center.
- Seek assistance from other investigators who specialize in technology-based crimes.
- Collaborate with your local County Attorney's Office.

Slide 15: Let's look at some legal considerations regarding devices:

- Seizing Devices

    - A device can be seized if you determine it contains evidence, which does not require a search warrant.
- Searching Devices
    - If seized, a device can't be searched until a legal basis is established. To search a device, you must first obtain written consent by the person who has a right to privacy, or you need a search warrant.
- Exigent Circumstances
    - If you demonstrate that exigent circumstances exist, such as evidence will be damaged, lost, or destroyed by waiting for a search warrant, then you may seize and search a device.

Slide 16: You should understand and consider the impact on a survivor if you take their device for evidence.

- The device may be the survivor's only means of communication with friends, family, children, work, or the outside world.
- The device may be the survivor's way of feeling safe after the assault.
- The survivor may go through physical or emotional withdrawals due to dependency to technology.
- The survivor may not have the financial means to replace the device.
- The device contains personal and private information of the survivor's life that could compromise the survivor.

Slide 17: You might need to request a **forensic analysis**, which requires:

1) Written consent from the device's owner with identifying information, including the device maker and model, serial number, device phone number, passcode/swipe code, service provider, or
2) A search warrant describing the detailed information you want to recover from the device.

Slide 18: Forensic analysis of any device should only be conducted by a specialized trained forensic examiner. The results of a forensic technological exam could include two different categories. Let's look at Android and Apple devices first:

Android and Apple devices	**Computers**
• Device information • Personal information, call logs, contacts, user accounts • Chats, emails, SMS and MMS, or Instant Messages • Search history and bookmarks • GPS information	• Device information • Chats, emails, and Instant Messages • Search history, search items, bookmarks, internet addresses, temporary internet files

• Images, Videos, Audio, Text • Applications • Documents	• Internet cache: a location on a computer where information may be previewed and saved • Programs installed and removed • Photos, Video, Audio, Text • Documents • Potentially deleted items • Other important data about the computer's operation

WARNING Connecting an external storage device to a computer adds and alters information on the device. It will not be considered unaltered evidence. Also, connecting the device may allow data to be erased by a remote user.

Back to Menu

Social Media

Slide 19: Social media is the use of websites and applications to create and share content with others to participate in social networking. Information documented on social media can include photos, videos, location, date, time, communications, and activities, often in real time. This information is often spontaneous, relatively permanent, and easily accessible. As an investigator, you should learn how to search for, identify, and harvest evidence from social media.

Slide 20: As of summer 2021, some of the most popular free Social Media platforms include:

- Facebook: a platform that allows registered users to share information, photos, videos, and messages with other users.
- Twitter: A micro-blogging service that allows registered users to broadcast short posts, called tweets, including pictures and videos to other members.
- Instagram: A social networking application made for sharing photos and videos from a handheld electronic device to other registered users.
- Discord: A VoIP, instant messaging, and digital distribution platform. Users communicate with voice and video calls, text messaging, media, and files in private chats or as part of communities called "servers," which are a collection of persistent chat rooms.
- YouTube: A popular video sharing website where registered users can upload and share videos with anyone able to access the information.
- Snapchat: A multimedia instant messaging app. Pictures and messages are usually only available for a short time before they become inaccessible to their recipient.
- TikTok: A video sharing network. This platform is used to make a variety of short-form videos that have a duration from 15 seconds to three minutes.

Slide 21: Keep in mind that the survivor and suspect may have interacted on an online dating website, and the website may contain valuable evidence and information. Here are just a few platforms:

- Bumble
- Plenty of Fish
- Match
- Tinder
- e-Harmony
- OKCupid

Slide 22: To identify evidence on social media sites, try to collect the following information:

- Email addresses
- Screen names and usernames
- Cell phone numbers
- Nicknames

Most of this information can be found using search sites, such as these:

- PIPL (www.pipl.com)
- Google (www.google.com)
- PeekYou (www.peekyou.com)
- Zabasearch (www.zabasearch.com)
- Spokeo (www.spokeo.com)

These kind of search sites may return additional useful information, such as profiles on social media sites or dating sites, as well as employment history, family members, addresses, news articles, public legal proceedings, and maybe uncover evidentiary items, such as videos, photos, messages, posts, or emails.

Slide 23: To collect social media evidence you should document the social media information on the screen by taking a screenshot. You can also execute a search warrant on ISPs or ESPs for more specific information.

- ISP stands for Internet Service Provider, which is any company that provides access to the internet for a fee, such as Spectrum, Charter, AT&T, or Comcast.
- ESP stands for Electronic Service Provider, which is any company that provides services for electronic communication, such as email, Facebook, YouTube, Amazon, or Craigslist.

Slide 24: Submit a request to the ISP or ESP provider as soon as possible, even on the day of the incident or report, to ensure the publicly shared evidence located during an internet search is not permanently deleted. Providers will keep content only for a few days. Understand a preservation request will only preserve evidence from the time of request and backward. Preservation requests cannot be made for anything in advance. A preservation request should contain:

- The cell phone number and potential identified user of the cell phone number.
- The email address and the email provider.
- The username or vanity name and the social media provider.

You need to know: You need to write specifically into the request or legal process that the notification of the account holder will jeopardize the investigation. Many ISP and ESP providers have a policy notifying the account holder, user, or cell phone owner that a preservation request has been made.

Slide 25: If you locate publicly shared evidence during an internet search, you can

1) Collect the evidence by simply printing out the internet page.
2) Use a screen capture tool to make a digital copy. Smartphones and computers have a "screenshot" feature that can capture an image of the screen. Use Google to search for instructions.
3) Take a photo to collect the evidence.

Always document in writing how you found and collected the evidence. To obtain more detailed evidence on or about social media accounts, you will need a subpoena or search warrant.

Slide 26: When requesting specific information from social media, a subpoena or search warrant is required. A subpoena allows an ESP or ISP to release:

1) Usernames
2) Potential physical addresses
3) Physical billing addresses
4) Mobile numbers
5) Registration Email addresses
6) Registration IP addresses
7) Log on IP addresses, including dates and times
8) Devices used to create profiles, accounts, and usernames

A search warrant allows an ESP or ISP provider to release

1) Protected electronic communication content, including:
    a. Email contacts
    b. Messaging services
    c. Documents
    d. Search terms
    e. Calendars
    f. Billing information
    g. Other saved data
2) Visual media including pictures and videos
3) Posted content

Visit www.SEARCH.org to access law enforcement guides for ESPs and the type of evidence available for collection with a subpoena or search warrant.

Slide 27: Document the name of the ESP or ISP employee (commonly called "Keepers of the Records") when:

- You serve a subpoena or search warrant

- You obtain the requested information

Slide 28: If the case is adjudicated, the records require certification in court from a designated ESP or ISP Keeper of records to certify

a) that the records were those requested by the officer and
b) the process of how the records were provided to the officer.

This is done by in-person testimony or by sworn affidavit.

Seek assistance from a forensic analyst or computer crimes investigator to fully understand ESP or ISP evidence.

Slide 29: As an Investigator, you are responsible for the handling of electronic evidence, particularly collection and storage. So, be aware of the legal processes for how to obtain the electronic evidence.

1) Subpoena: requires a return-of-service affidavit.
    a. Subpoenaed electronic evidence is usually returned via email or postal mail, with limited results.
    b. You should document in a supplemental report when the results were returned.
2) Search Warrant requirements:
    a. A *Search Warrant Return* documents:
        i. How the search warrant was served.
        ii. Person or entity that was served the search warrant.
        iii. When the search warrant was served.
        iv. Who served the search warrant.
    b. A *Search Warrant Receipt* documents:
        i. What is being requested.
        ii. How the evidence will be delivered.
        iii. What the evidence consists of.
        iv. When the evidence was received.
    c. A *Custody Order and Disposition*: authorizing evidence storage and dissemination.

Slide 30: Once you have obtained the electronic evidence, you should:

1) Verify what you received was in fact the information you requested.
2) Document in a supplemental report when the evidence was received.
3) Document that all electronic evidence was viewed.
4) Document that the electronic evidence was secured according to agency policy.
5) Understand that the evidence may depict sensitive material and should not be shared with unauthorized individuals.

Back to Menu

Quiz

Slide 31: Let's test what you've learned. Take the quiz on the following pages to test your knowledge.

Slide 32: Multiple Choice: What type of device should you consider as possible digital evidence? (Mark all that apply)

- ☑ A) Smart Phone
- ☑ B) Computer
- ☑ C) Fitbit
- ☑ D) Thumb Drive
- ☑ E) iPod
- ☐ F) Houseplant

Correct Answer: That's right. Anything with an on and off switch is a potential source or evidence, but in this case particularly a smart phone, computer, Fitbit, thumb drive, and iPod. Click anywhere to continue.

Incorrect Answer: That's incorrect. Anything with an on and off switch is a potential source or evidence, but in this case particularly a smart phone, computer, Fitbit, thumb drive, and iPod. Click anywhere to continue.

Slide 33: Correct or Incorrect: Once a device is collected as evidence, you need to observe any information on the display, place the device into a mode that will not transmit data, and provide the owner with a property receipt that identifies the device.

- ☑ A) Correct
- ☐ B) Incorrect

Correct Answer: That's correct! First and foremost, observe any information on the display, which is considered plain view and may be excluded from the search warrant requirement. Then, place the device into a mode that will not transmit data, such as airplane mode, disabling the Wi-Fi, powering down the device, or even removing the battery, if easily accessible, to keep evidence from being destroyed remotely. And finally, provide the owner with a property receipt that identifies the device. Click anywhere to continue.

Incorrect Answer: That's not quite right. First and foremost, observe any information on the display, which is considered plain view and may be excluded from the search warrant requirement. Then, place the device into a mode that will not transmit data, such as airplane mode, disabling the Wi-Fi, powering down the device, or even removing the battery, if easily accessible, to keep evidence from being destroyed remotely. And finally, provide the owner with a property receipt that identifies the device. Click anywhere to continue.

Slide 34: Multiple Choice: How do you store digital evidence correctly? (Mark all that apply)

- ☑ A) Place the device into a container, such as a manila envelope or Ziploc bag.

- ☑ B) Ensure the device is properly packaged and buffered.
- ☑ C) Seal the container with evidence tape, initial the evidence tape, and write the date, case number, description of the evidence, and the property owner's name on the container.
- ☑ D) Attach an evidence tag.
- ☑ E) Place the device into a proper evidence receptacle.
- ☑ F) Consider a Faraday bag if there is any risk the device may transmit or be compromised by outside sources.

Correct Answer: That's right. You store digital evidence correctly by placing the device into a container, such as manila envelope or Ziploc bag. Ensure the device is properly packaged and buffered. Seal the container with evidence tape, initial the evidence tape, and write the date, case number, description of the evidence, and the property owner's name on the container. Attach an evidence tag. Place the device into a proper evidence receptacle. And consider a Faraday bag if there is any risk the device may transmit or be compromised by outside sources. Click anywhere to continue.

Incorrect Answer: No, that's incorrect. You store digital evidence correctly by placing the device into a container, such as manila envelope or Ziploc bag. Ensure the device is properly packaged and buffered. Seal the container with evidence tape, initial the evidence tape, and write the date, case number, description of the evidence, and the property owner's name on the container. Attach an evidence tag. Place the device into a proper evidence receptacle. And consider a Faraday bag if there is any risk the device may transmit or be compromised by outside sources. Click anywhere to continue.

Slide 35: True or False: You don't have to worry about the survivor if you take their device for evidence.

- ☐ True
- ☑ False

Correct Answer: You're right! You should understand and consider the impact on a survivor if you take the device for evidence. The device may the survivor's only means of communication with friends, family, children, work, or the outside world. It might also make the survivor feel safe after the assault. In addition, device withdrawal can be a real problem and the survivor may go through physical or emotional withdrawals. The survivor may not have the financial means to replace the device. And the device may contain personal and private information of the survivor's life that could compromise them. Click anywhere to continue.

Incorrect Answer: No, that's incorrect. You should understand and consider the impact on a survivor if you take the device for evidence. The device may the survivor's only means of communication with friends, family, children, work, or the outside world. It might also make the survivor feel safe after the assault. In addition, device withdrawal can be a real problem and the survivor may go through physical or emotional withdrawals. The survivor may not have the financial means to replace the device. And the device may contain personal and private information of the survivor's life that could compromise them. Click anywhere to continue.

Slide 36: Multiple Choice: When requesting specific information from social media, a subpoena or search warrant is required. A subpoena allows an ESP or ISP to release: (mark all that apply)

- ☑ A) Usernames
- ☑ B) Potential physical addresses
- ☑ C) Mobile numbers
- ☑ D) Registration Email and IP addresses
- ☑ E) Log on IP Addresses, including dates and times
- ☑ F) Devices used to create profiles, accounts, and usernames
- ☐ G) Personal Identifying Information about family members

Correct Answer: Yes, that's right. A subpoena allows an ESP or ISP to release usernames, potential physical addresses, mobile numbers, registration email and IP addresses, log on IP addresses, including dates and times, and information about devices used to create profiles, accounts, and usernames. Click anywhere to continue.

Incorrect Answer: No, that's not quite right. A subpoena allows an ESP or ISP to release usernames, potential physical addresses, mobile numbers, registration email and IP addresses, log on IP addresses, including dates and times, and information about devices used to create profiles, accounts, and usernames. Click anywhere to continue.

Slide 37: Quiz Results

Slide 38: In this course you have learned about the different types of technology and social media platforms and how to identify and collect digital evidence.

Slide 39: Thank you for completing this course. Select "Close" to exit.
Back to Menu