WHAT IS DIGITAL FORENSICS?

Rachael Elliott, M.S.

University of Central Oklahoma - Forensics Science Institute

Edmond Police Department Digital Crime Lab

DIGITAL FORENSICS DEFINED

- The field of forensic science that is concerned with retrieving, storing and analyzing electronic data that can be useful in criminal investigations. (NIST)
- Includes, but not limited to, computers, networks, cloud data and mobile devices
- Purpose is to uncover evidence for criminal or civil investigations
- It ensures evidence integrity and admissibility in court through strict, validated, and repeatable methods

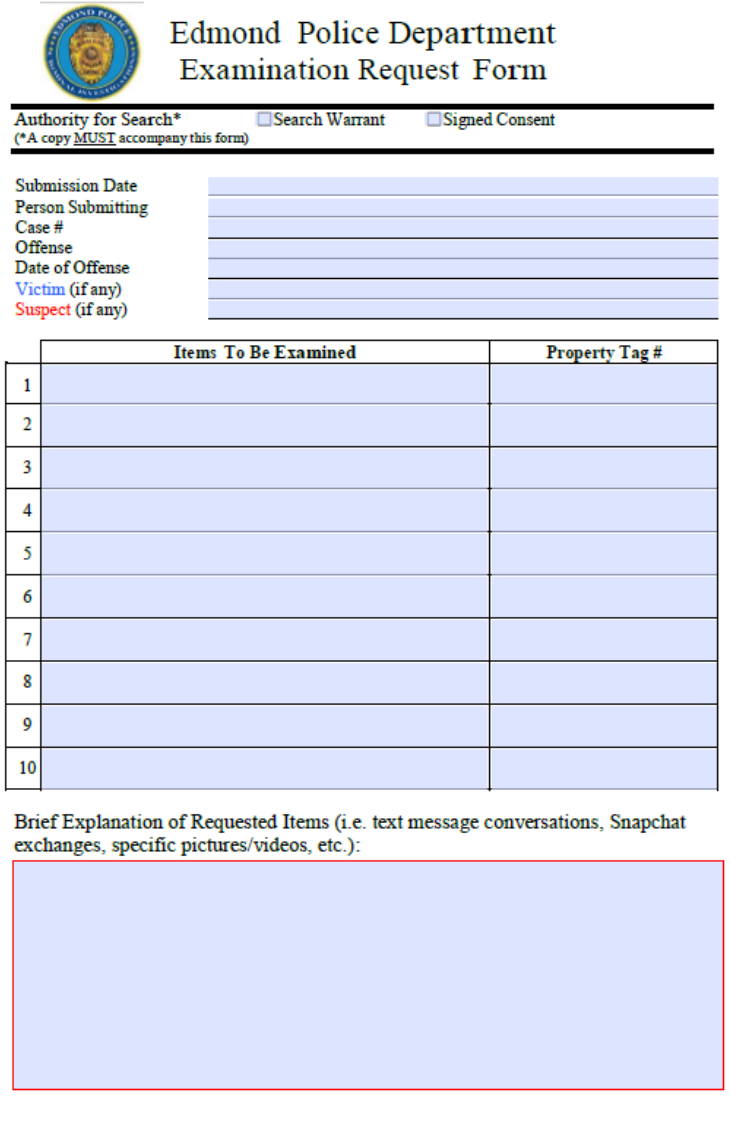
ORGANIZATIONS OF NOTE

- International Association of Computer Investigative Specialists (IACIS)
- Scientific Working Group on Digital Evidence (SWGDE)
- National Institute of Standards and Technology (NIST)
- American Academy of Forensic Sciences (AAFS)

THE DIGITAL FORENSICS PROCESS

REQUEST FOR EXAMINATION

- Digital devices that have been seized with proper search authority are brought to the digital lab for analysis
- A "Request for Examination" form is completed by the investigator/detective
- This information assists with the assessment phase



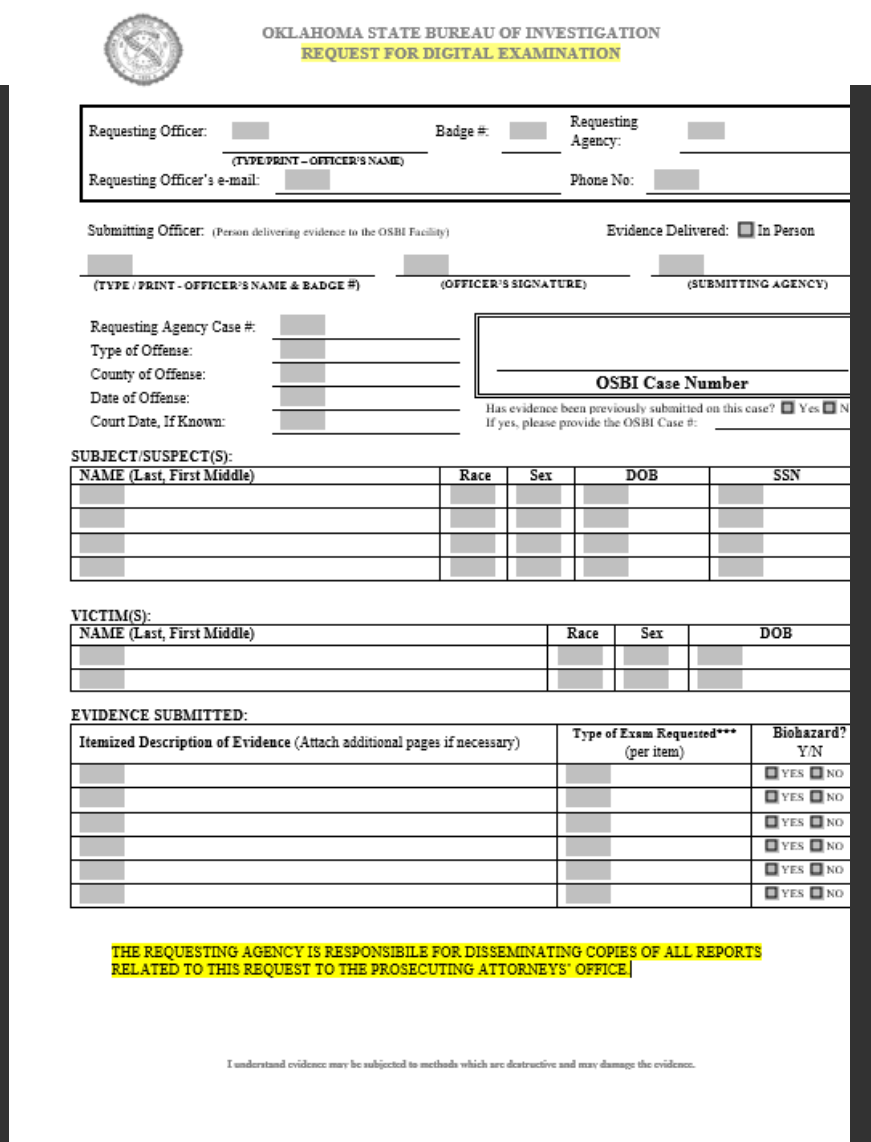
Edmond Police Department
Examination Request Form

Authority for Search* ☐ Search Warrant ☐ Signed Consent
(*A copy MUST accompany this form)

Submission Date
Person Submitting
Case #
Offense
Date of Offense
Victim (if any)
Suspect (if any)

	Items To Be Examined	Property Tag #
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Brief Explanation of Requested Items (i.e. text message conversations, Snapchat exchanges, specific pictures/videos, etc.):



OKLAHOMA STATE BUREAU OF INVESTIGATION
REQUEST FOR DIGITAL EXAMINATION

Requesting Officer: Badge #: Requesting Agency:
(TYPE/PRINT – OFFICER'S NAME)
Requesting Officer's e-mail: Phone No:

Submitting Officer: (Person delivering evidence to the OSBI Facility) Evidence Delivered: ☐ In Person
(TYPE / PRINT - OFFICER'S NAME & BADGE #) (OFFICER'S SIGNATURE) (SUBMITTING AGENCY)

Requesting Agency Case #:
Type of Offense:
County of Offense:
Date of Offense:
Court Date, If Known:

OSBI Case Number
Has evidence been previously submitted on this case? ☐ Yes ☐ N
If yes, please provide the OSBI Case #:

SUBJECT/SUSPECT(S):

NAME (Last, First Middle)	Race	Sex	DOB	SSN

VICTIM(S):

NAME (Last, First Middle)	Race	Sex	DOB

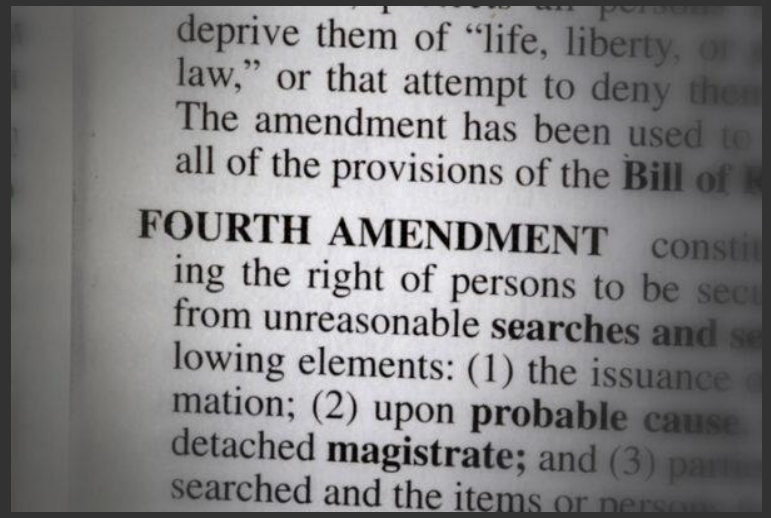
EVIDENCE SUBMITTED:

Itemized Description of Evidence (Attach additional pages if necessary)	Type of Exam Requested*** (per item)	Biohazard? Y/N
		☐ YES ☐ NO
		☐ YES ☐ NO
		☐ YES ☐ NO
		☐ YES ☐ NO
		☐ YES ☐ NO
		☐ YES ☐ NO

THE REQUESTING AGENCY IS RESPONSIBILE FOR DISSEMINATING COPIES OF ALL REPORTS RELATED TO THIS REQUEST TO THE PROSECUTING ATTORNEYS' OFFICE.

I understand evidence may be subjected to methods which are destructive and may damage the evidence.

ASSESSMENT

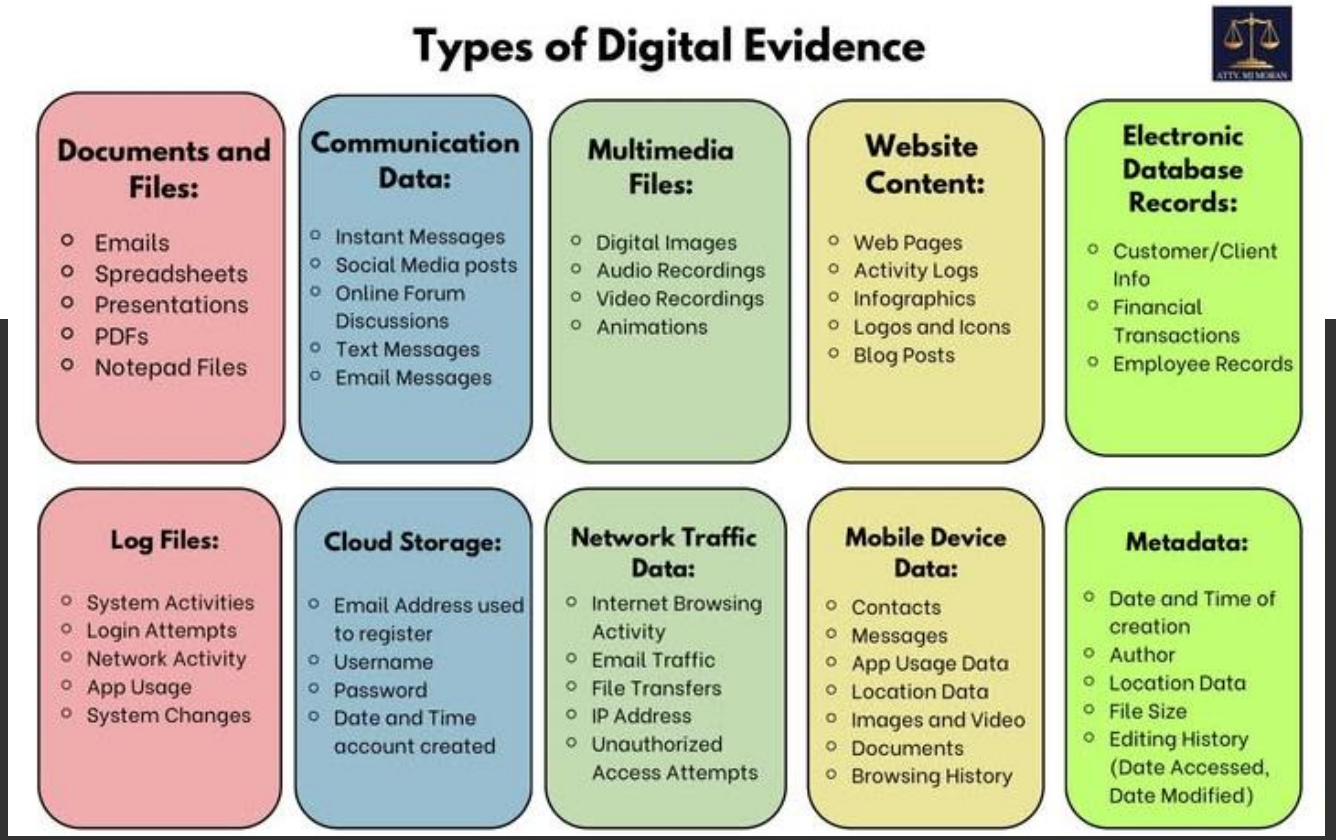

deprive them of "life, liberty, or
law," or that attempt to deny them
The amendment has been used to
all of the provisions of the **Bill of**

FOURTH AMENDMENT consti
ing the right of persons to be secu
from unreasonable **searches and** se
lowing elements: (1) the issuance
mation; (2) upon **probable cause**
detached **magistrate;** and (3) par
searched and the items or person

- Do we have proper search authority?
- What evidence devices were submitted?
  - Computers, laptops, cell phones, USB devices, memory cards, cameras, etc.
  - Are there additional sources of evidence? (Cloud, social media, call detail records, etc.)

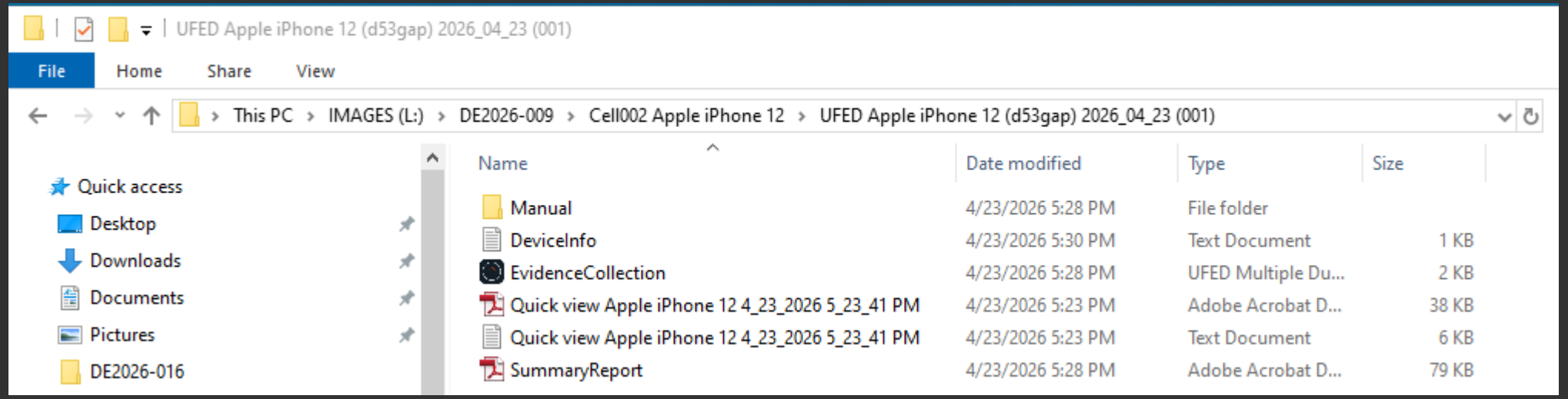
ASSESSMENT

- What types of data/evidence are we looking for?
- What forensic tools are needed for acquisition and analysis?
- What is the priority order of the devices submitted to the lab?

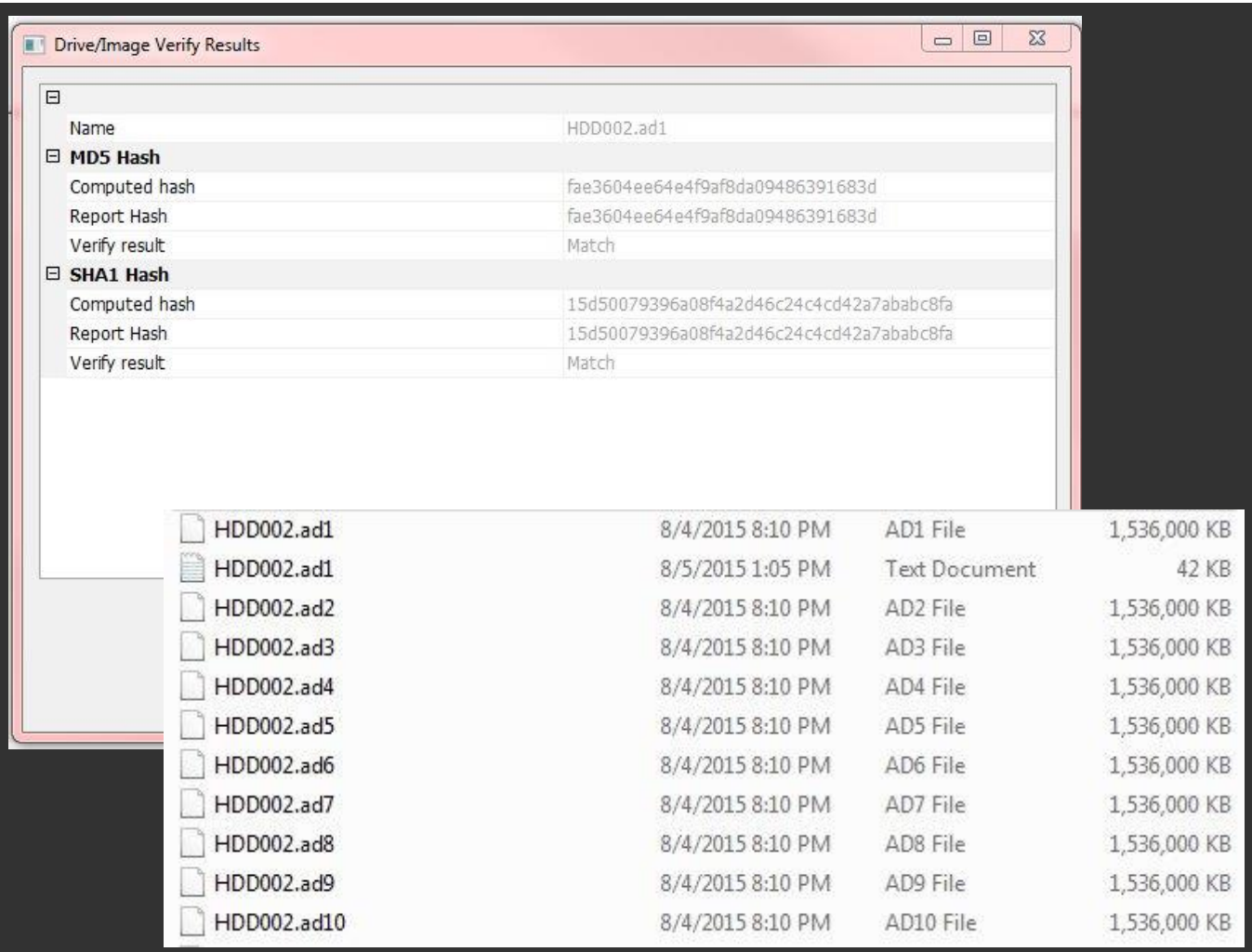


ACQUISITION

- Digital examiners do not conduct examinations using the original device, as a general rule…this ensures data integrity.
- An acquisition of data contained on a mobile device is conducted and all analysis is performed on the acquired data.



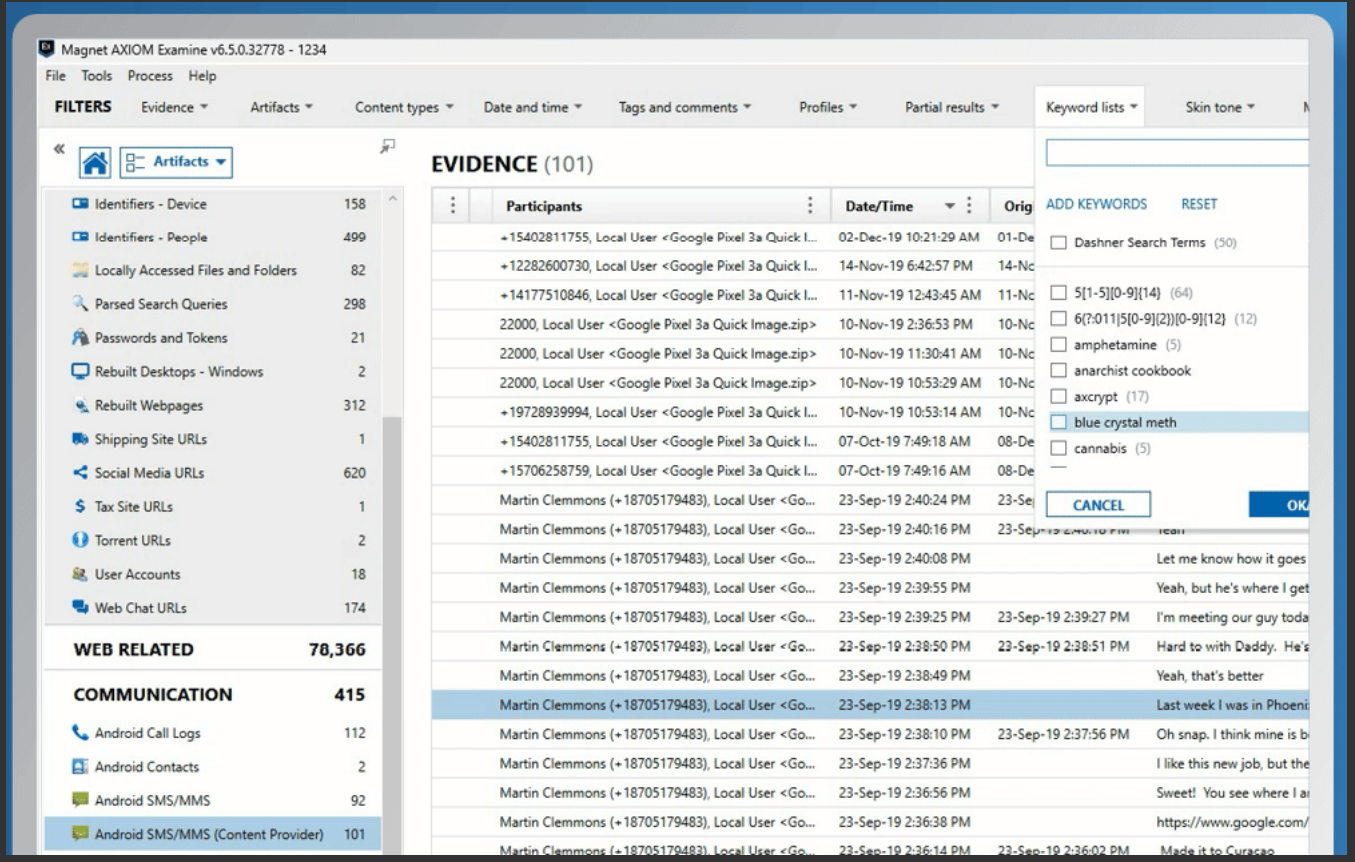
IMAGING

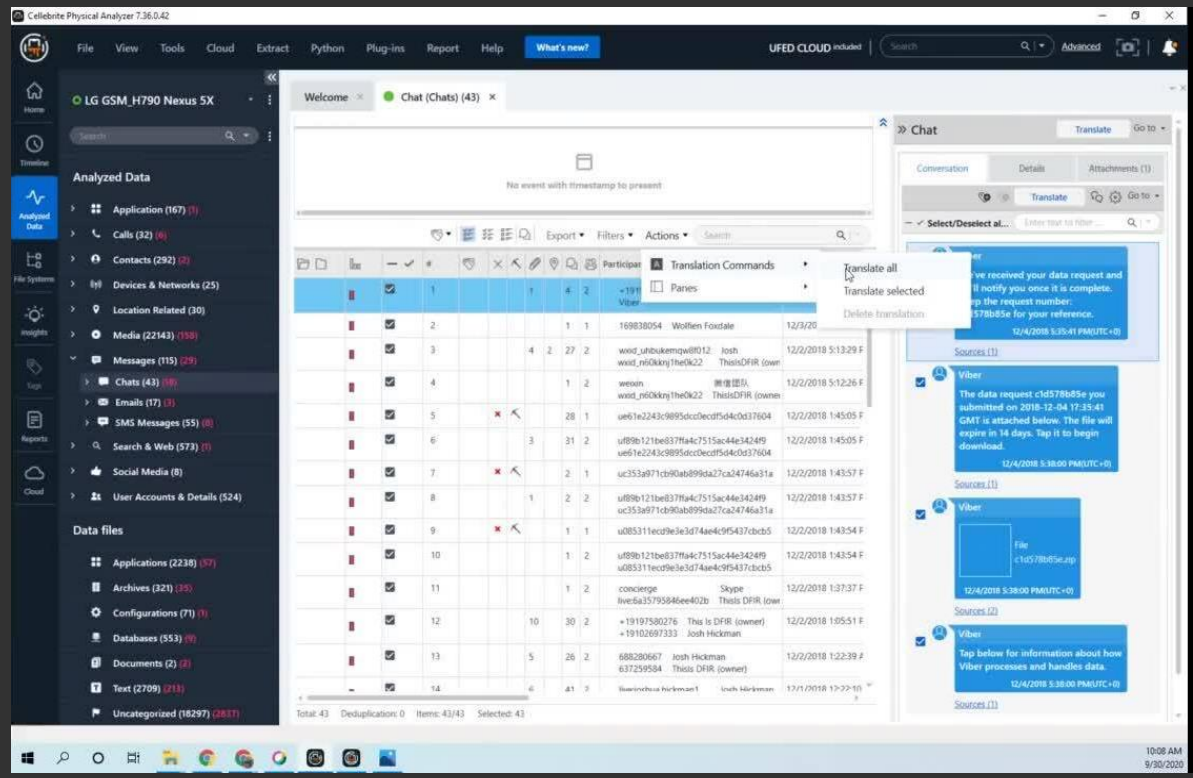


- A forensic image is obtained for all hard drives, SSDs, USBs, memory cards, etc.
- A forensic image is a file or group of files that is a bit for bit copy of all the data contained on the device.
  - This includes active data, partially overwritten data, and deleted data
- The forensic image is verified as a true and accurate copy by utilizing hash values
  - It is recommended that multiple hashing algorithms are utilized to ensure a collision has not occurred.

EXAMINATION

- NIST defines examination as searching for data, recovering hidden/deleted files, and identifying relevant information using validated tools.





EXAMINATION

- While the forensic images and data acquisitions from digital devices contain most/all data contained on the device, examiners must ensure they are staying within the scope of the search authority.
- Important for investigators to include this information in the request forms for examiners.
- It is important to understand that the software generated reports, while detailed, only report the data and do not include explanations of the data and are not designed to stand on their own.

Forensic Science Instute DEU Request Form For Classroom Use ONLY

Authority for Search* ■Search Warrant ☐Signed Consent
(*A copy MUST accompany this form)

Submission Date	
Person Submitting	Det. John Smith
Case #	CR#001
Offense	Rape
Date of Offense	4/10/2011
Victim (if any)	Crystal Bloom
Suspect (if any)	Don Johnson

	Items To Be Examined	Property Tag #
1	Black 4GB flash drive	1
2		
3		
4		
5		
6		
7		
8		
9		
10		

Brief Explanation of Requested Items (i.e. text message conversations, Snapchat exchanges, specific pictures/videos, etc.):

The victim claims the suspect had been following her around for weeks. He was seen outside her home and the gym where she was known to work out. The victim knows the suspect from work. They were at a work event when she began feeling strangely but reports she had not been drinking. The last thing she remembers is walking out to her car to go home but she woke up at her home, located at 9605 Willow Wind Drive not wearing any clothes and her car was not there. Her blood toxicology showed she had Rohypnol in her system. Her car was found to be still parked at her job. She has no memory of seeing anyone at her car the night before or at her home the next morning, but the neighbors report witnessing a car leaving her home early that morning while it was still dark matching the type driven by Mr. Johnson. In his interview he claims he is innocent, and that he didn't even know where she lives.

FORENSIC EXAMINATION REPORT

CASE NUMBER CAPSTONE

Organization	UCO Forensic Science Institute
Examiner	Rachael Elliott
Case generated	Monday, February 16, 2026
Report generated	Monday, February 23, 2026

Record	Tags	Comments	Item	Artifact type	Artifact category	Date and time	Source	Location
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	• Bookmark		GreenQueens	User Accounts - Windows	Operating System	10/5/2021 1:57:44.000 PM	• HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SAM • HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SOFTWARE	• Registry Key: SAM\Domains\Account\Users\000003E9 • Registry Key: SAM\Domains\Builtin\Aliases\00000220 • Registry Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2108979123-2695303068-2107575892-1001
2	• Bookmark		Willow	User Accounts - Windows	Operating System	10/4/2021 8:03:11.000 PM	• HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SAM • HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SOFTWARE	• Registry Key: SAM\Domains\Account\Users\000003EA • Registry Key: SAM\Domains\Builtin\Aliases\00000221 • Registry Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2108979123-2695303068-2107575892-1002
3	• Bookmark		William	User Accounts - Windows	Operating System	10/4/2021 6:06:59.000 PM	• HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SAM • HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SOFTWARE	• Registry Key: SAM\Domains\Account\Users\000003EB • Registry Key: SAM\Domains\Builtin\Aliases\00000221 • Registry Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2108979123-2695303068-2107575892-1003
4	• Bookmark		User Accounts	User Accounts	Refined Results		• HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SAM • HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SOFTWARE	• Registry Key: SAM\Domains\Account\Users\000003E9 • Registry Key: SAM\Domains\Builtin\Aliases\00000220 • Registry Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2108979123-2695303068-2107575892-1001
5	• Bookmark		User Accounts	User Accounts	Refined Results		• HD001.E01 - Partition 2 (Microsoft NTFS, 36.7 GB)\Windows\System32\config\SAM • HD001.E01 - Partition 2 (Microsoft NTFS, 36.7	• Registry Key: SAM\Domains\Account\Users\000003EB • Registry Key: SAM\Domains\Builtin\Aliases\00000221 • Registry Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2108979123-

Pictures

Search:

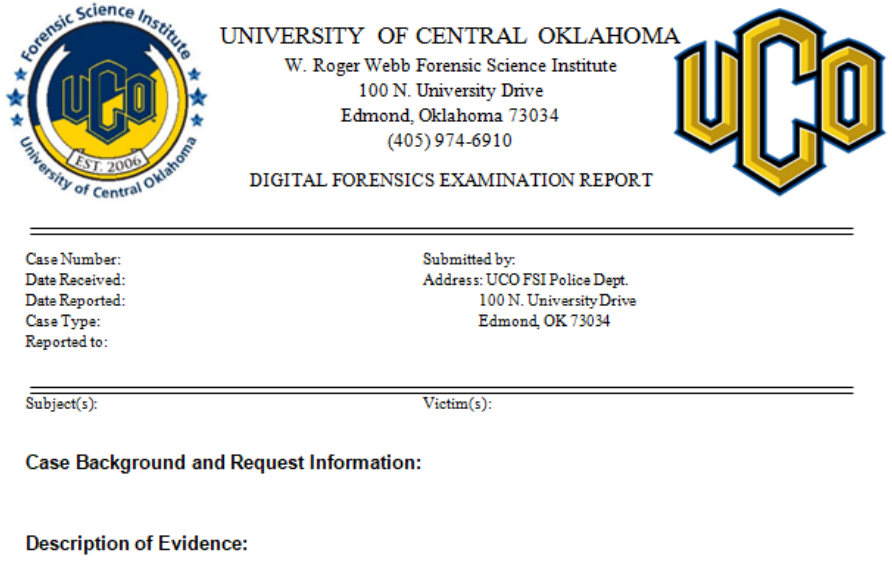
Image	File Name	File Extension	Created Date/Time - UTC+00:00 (M/d/yyyy)	Last Accessed Date/Time - UTC+00:00 (M/d/yyyy)	Last Modified Date/Time - UTC+00:00 (M/d/yyyy)	Size (Bytes)	Skin Tone Percentage	Original Width	Original Height	Exif Extraction Status	Creat Date/ - Loc Time (yyyy dd)
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filte
	19710810_171545.jpg	.jpg	8/28/2020 8:39:47.976 PM	10/5/2021 2:00:34.887 PM	8/10/1971 10:15:45.000 PM	2714986	42.0	3264	1836	Complete	1971 17:15

Contents

Type	Included in report	Total
Chats	1	1
Native Messages	1	2
Contacts	4	4
Device Info	48	48
Installed Applications	2	2
User Accounts	9	9
Data Files	1	1
Databases	1	1
Tagged items	65	65

2	OneTravel **Application ID:** EEA397B3-BC62-4EA6-A28E-A45CF93E730A com.99taxis **Source:**	**Version:** **Operation Mode:** Foreground **Application Size (bytes):** 0 --- **Source Extraction:** Logical **Artifact Family:** **Source Repository Path:**	**Purchase Date** **Install Date** **Last Modified** **Deleted Date**				**Launches** **Activations** **Last Launch Active Time** 00:00:00 **Background Time** 00:00:00	**Categories** LIFESTYLE		

Name	Description	Timestamp	Copyright	Permissions	Alias names	App usage	App categories	Deleted
Dingtone **Application ID:** 17EC71B1-5AE0-4DC2-8F10-CD02B85F98E5 me.dingtone.im **Source:**	**Version:** **Operation Mode:** Foreground **Application Size (bytes):** 0 --- **Source Extraction:** Logical **Artifact Family:** **Source Repository Path:**	**Purchase Date** **Install Date** **Last Modified** **Deleted Date**		Contacts Photos		**Launches** **Activations** **Last Launch** **Active Time** 00:00:00 **Background Time** 00:00:00	**Categories** SPOOFING SOCIAL_NETWORKING	



UNIVERSITY OF CENTRAL OKLAHOMA
W. Roger Webb Forensic Science Institute
100 N. University Drive
Edmond, Oklahoma 73034
(405) 974-6910

DIGITAL FORENSICS EXAMINATION REPORT

Case Number:
Date Received:
Date Reported:
Case Type:
Reported to:

Submitted by:
Address: UCO FSI Police Dept.
100 N. University Drive
Edmond, OK 73034

Subject(s):

Victim(s):

Case Background and Request Information:

Description of Evidence:

Results of Examination:

[HD001]

Forensic Image Date:
Original MD5 Hash Value:
Image MD5 Hash Value:
Original SHA1 Hash Value:
Image SHA1 Hash Value:

OS:
Registered Owner:
Last Shutdown Time:

Installed:
Computer Name:
Timezone:

User Accounts:

User Name	SID	Last Written (UTC)	Last Logon (UTC)	PW Required

*Other standard user accounts were listed within the registry, however they were not active.

Report Summary:

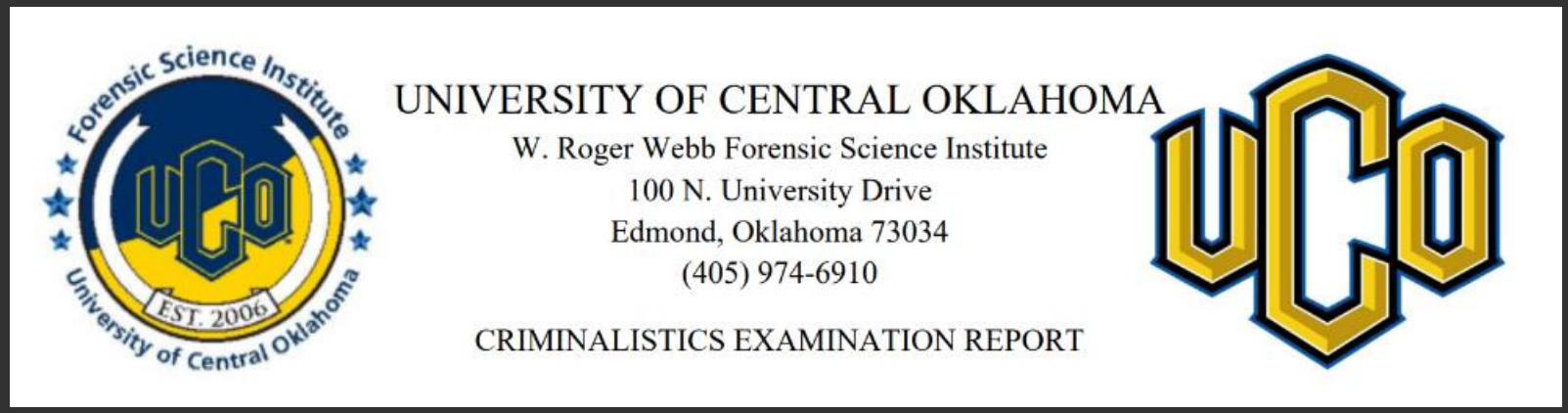
FOR CLASSROOM PURPOSES ONLY

REPORTING

- NIST defines analysis as interpreting the data to determine its significance, such as timelines of activity or identifying owners.
- This is where the examiner creates a narrative, or examiner's report, that explains in detail the data included in the software generated report files, including, but not limited to:
  - Identity of Reporting Agency
  - Case Number
  - Identity of submitting person/case investigator
  - Dates of receipt/request
  - Detailed description of the evidence items
  - Identity of the examiner
  - Description of steps taken during examination process
  - Results and conclusions

EXAMINER'S REPORT

- This report should explain how the data connects to the investigation and assists in proving the elements of the crime.
- This report often cannot place anyone "at the keyboard," but efforts should be made to identify ownership of the device.
- This report should be written in a way that non-technical people (judges, attorneys, investigators, and jury members) can understand.
- Should only contain information the data can support, no opinions or unsubstantiated conclusions



Examiner's Report

Examiner: Rachael Elliott
Requesting Agency: Forensic Science Institute
Contact Info: Detective Sam Winchester
Agency Case#: 2021-01522
Examiner's Case#: DE2021-001

On 2/16/2026, Detective Sgt. Sam Winchester requested my assistance with the forensic examination of digital evidence devices in a cold case homicide investigation. These devices were seized during the execution of a search warrant at the suspect's residence, 5148 Louise Ave. in Edmond, Oklahoma on 10/16/2021. Det. Winchester provided a signed, Oklahoma County search warrant for the forensic examination of a Dell Optiplex 390 computer (HD001) and an Apple iPhone 5c (Cell001). This investigation began on 10/4/2021 at 1731 hours when Edmond Police Department received a 911 call reporting the victim, Jessica Pratt, had been found unresponsive in the backyard of her residence by her husband, William Pratt. According to the search warrant affidavit, surveillance footage recorded by the Ring doorbell camera across the street from the victim's residence show a white Kia Soul with Oklahoma license plate XLY269 stopping in front of 1627 Revello Dr. on 10/4/2021 at 0903 hours, which is the residence across the street from the victim's home. Further investigation determined the vehicle was registered to Thomas Wayne Harris. During an interview with Mr. Harris, he stated he was a driver for a rideshare application named 99 Private Driver and Taxi App. He went on to state he picked up a customer by the name of Willow Rosenboom that morning and admitted to dropping her off at that location. He describes Willow as a petite, blonde wearing a white t-shirt and jeans. He was able to provide a receipt confirming this information and a subsequent receipt showing he left the area to immediately pick up his next customer. According to Det. Winchester, Willow Rosenboom is a business partner of Green Queens dispensary with the victim. Early examination of the victim's cell phone show text exchanges between a phone number identified as Ms. Rosenbloom's and the victim arguing about money. In this text exchange, these individuals agreed to meet at approximately 0900 on 10/4/2021. Additionally, Det. Winchester advised there was a history of domestic violence between the victim and her husband, Mr. William Pratt. He also advised that Willow Rosenbloom's father was identified as Mitchell Luciano, the head of a well-known organized crime family.

Digital Crime Lab Examinations

A forensic image of the data contained on the hard drive removed from the Dell Optiplex 390 computer was created using AccessData® FTK® Imager version 4.5.0.3. This

QUESTIONS?