|  |  |
| --- | --- |
| **STATE OF {stateUpper}**  **{**county**} County** | **)**  **) SS: In the {county} {**courtType**} Court**  **)** |

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

The Undersigned Affiant swears upon their oath that they believe and have good cause to believe that certain evidence involved in the commission {offenseType}, in violation of {state} Code {violationCode}, which are believed to be concealed on or about the following digital device, to wit: {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers}.

### PROPERTY DESCRIPTION

1. {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers}
2. Photos of the {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers} are as follows:

{#images}  
{%image}  
{/}

**EVIDENCE SOUGHT**

1. For the {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers}, between the dates of {startDate} and {endDate}, the following digitally stored evidence related to the crime of {offenseType}:

**Evidence Sought:**

{#evidenceSought}

* {.}

{/evidenceSought}

**Evidence NOT Sought:**

{#evidenceNotSought}

* {.}

{/evidenceNotSought}

**INTRODUCTION AND INVESTIGATOR BACKGROUND**

I, {userName}, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

1. I am a sworn police investigator employed by the {userDepartment}. In my current position, I am a {userPosition}{#hasUnit} with the {userUnit}{/hasUnit}.
2. {userBackground}
3. I make this affidavit in support of probable cause for a search warrant to search a {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers} for digital evidence, between the dates of {startDate} and {endDate}, related to the crime of {offenseType}.

**APPLICABLE DEFINITIONS**

1. Web Related evidence pertains to digital artifacts extracted from the internet, shedding light on an individual's online activities. This encompasses a range of elements, such as visited websites, conducted searches, downloaded files, bookmarked webpages, cookies, and records of viewed content stored on their computer.
2. Communication evidence is any information that shows how someone has talked to or communicated with someone else. This could include things like phone calls, email addresses, text messages, social media messages, or even contacts. It can also include things like recordings of conversations or screenshots of messages. Communication evidence can be used to indicate that someone talked to someone else, or to find out what they talked about. It can also be used to find out when someone talked to someone else, or how often they talked.
3. Social networking evidence is any information that is stored on social media websites or applications. This could include things like posts, profiles, friends, and messages. Social networking evidence can be used to prove that someone was at a certain place, or that they knew someone else. It can also be used to find out what someone was thinking or what they were doing.
4. Media evidence refers to audio or video information stored in various formats such as recordings, pictures, screenshots, and videos. It serves the purpose of demonstrating occurrences or determining events that took place. Additionally, media evidence aids in identifying individuals involved in incidents or ascertaining their actions.
5. Email and calendar evidence encompass information stored within email and calendar programs. This comprises email messages, attachments, and calendar events. Such evidence serves to establish actions undertaken by individuals or to ascertain the specifics of those actions. Moreover, it aids in identifying parties involved or determining the timing of events.
6. Documents evidence encompasses information stored in various document formats, including word processing documents, text files, spreadsheet files, presentation files, and user-created notes. It serves the purpose of demonstrating occurrences or determining events that took place. Additionally, document evidence aids in identifying individuals involved in incidents or ascertaining their actions.
7. Cloud Storage evidence includes files uploaded to online storage websites such as iCloud, Google Drive, and Dropbox that are saved and accessible on the phone.
8. Application Usage evidence refers to information that reveals the installed programs and applications on an individual's computer, the permissions granted to them, and their usage patterns. This evidence can establish the utilization of specific programs or applications or shed light on the activities performed within them. Furthermore, it can aid in identifying the party responsible for installing a particular program or application and determining the permissions assigned to it.
9. Operating System evidence encompasses information that provides insights into the functioning of a computer or mobile device. This evidence includes details such as the file system, owner information, configured accounts, cell tower and Wi-Fi connections, as well as device state information like time settings, battery level, and lock state.
10. Encryption & Credentials evidence encompasses information related to how individuals safeguard their files and accounts. This evidence includes encrypted files, password-protected files, as well as user login names, passwords, and tokens used to access user accounts.
11. Connected Devices evidence refers to information that demonstrates how individuals utilize their Internet of Things (IoT) devices. This evidence includes data such as the timestamp and duration of device connections, geographical locations, and transferred data. Connected devices encompass a range of examples, such as Amazon Alexa, Apple Watch, Fitbit, Nest, Bluetooth devices, and also encompass relevant details about the device's SIM card.
12. Location and travel evidence encompasses various types of information that shed light on an individual's whereabouts. Historical GPS locations reveal the past tracking of a device's GPS, providing insights into their previous locations. Map searches offer data on locations searched for using map applications, indicating areas of interest, or intended destinations. Significant locations denote places marked as significant by the device, which may include frequently visited spots like home, school, or workplace. Wi-Fi locations comprise information about Wi-Fi networks recognized or connected to by the device, as these networks are often specific to certain places such as coffee shops, libraries, or schools. Lastly, rideshare application data discloses details about rides taken using rideshare services, enabling the determination of specific locations visited as rides typically have identifiable start and end points. Collectively, these sources of evidence help establish a comprehensive understanding of an individual's movements and travel patterns.
13. Peer to Peer evidence includes data related to direct file access and sharing. This may include direct online payments between users or sharing videos and images through torrent websites.

**FACTS OF THE CURRENT INVESTIGATION**

{#userInvestigationFactsList}

1. {.}

{/userInvestigationFactsList}

1. Based on this information, I am requesting authorization to search the {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers}, between the dates of {startDate} and {endDate}, for the following digital evidence related to the crime of {offenseType}:
2. Web Related evidence. I believe there to be probable cause that the device contains Web Related evidence due to the following facts. {userProbableWebRelatedDevice}
3. Communication evidence. I believe there to be probable cause that the device contains Communication evidence due to the following facts. {userProbableCommunication}
4. Social Networking evidence. I believe there to be probable cause that the device contains Social Networking evidence due to the following facts. {userProbableSocialNetworking}
5. Media evidence. I believe there to be probable cause that the device contains Media evidence due to the following facts. {userProbableMediaEvidence}
6. Email & Calendar evidence. I believe there to be probable cause that the device contains Email & Calendar evidence due to the following facts. {userProbableEmailCalendar}
7. Documents evidence. I believe there to be probable cause that the device contains Documents evidence due to the following facts. {userProbableDocuments}
8. Cloud Storage evidence. I believe there to be probable cause that the device contains Cloud Storage evidence due to the following facts. {userProbableCloudStorage}
9. Application Usage evidence. I believe there to be probable cause that the device contains Application Usage evidence due to the following facts. {userProbableApplicationUsage}
10. Operating System evidence. I believe there to be probable cause that the device contains Operating System evidence due to the following facts. {userProbableOperatingSystem}
11. Encryption & Credentials. I believe there to be probable cause that the device contains Encryption and Credentials evidence due to the following facts. {userProbableEncryptionCredentials}
12. Connected Devices evidence. I believe there to be probable cause that the device contains Connected Devices evidence due to the following facts. {userProbableConnectedDevices}
13. Location & Travel evidence. I believe there to be probable cause that the device contains Location & Travel evidence due to the following facts. {userProbableLocationTravel}
14. Peer to Peer evidence. I believe there to be probable cause that the device contains Peer to Peer evidence due to the following facts. {userProbablePeerToPeer}

Based upon the foregoing facts as well as the training and experience of this Affiant, I believe there to exist the above listed items of evidence inside the {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers}.

I affirm under the penalties for perjury, that to the best of my personal knowledge and belief that the foregoing representations are true.

*{userSignature}*

{userPosition}, {userName}

{#hasUnit}{userUnit}{/hasUnit}

{userDepartment}

{userDepartmentAddress}

{userEmail}

{userTodayDate}

|  |  |
| --- | --- |
| **STATE OF {stateUpper}**  **{**county**} County** | **)**  **) SS: In the {**county**} {**courtType**} Court**  **)** |

**{userDepartment} Case # {caseNumber}**

TO: ANY CONSTABLE, POLICE OFFICER, SHERIFF, OR CONSERVATOR OF THE PEACE

GREETINGS:

WHEREAS, there has been filed with me an AFFIDAVIT, a copy of which is attached hereto and incorporated herein by reference; and

WHEREAS, there exists probable cause to believe that

For the {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers}, between the dates of {startDate} and {endDate}, the following digitally stored evidence related to the crime of {offenseType}:

**Evidence Sought:**

{#evidenceSought}

{.}

{/evidenceSought}

**Evidence NOT Sought:**

{#evidenceNotSought}

{.}

{/evidenceNotSought}

are located in/on/upon:

1. {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers}
2. Photos of the {deviceColor}, {deviceMake} {deviceModel} with {otherDeviceIdentifiers} are as follows:

{#images}  
 {%image}  
 {/}

YOU ARE THEREFORE ORDERED AND COMMANDED, in the name of the State of {state}, with the necessary and proper assistance, in the daytime or in the nighttime, to enter into or upon the electronic and digital storage items described herein, and diligently search for said items described herein related to the offense of {offenseType}, a violation of {state} Code {violationCode}, and bring you the same, or any part thereof found in the search, forthwith before me in the {county} {courtType} Court to be disposed of according to law. For the search of digital storage items, the search is limited to data between the dates of {startDate} and {endDate}.

GIVEN UNDER MY HAND AND SEAL, this \_\_\_\_\_\_\_ Day of \_\_\_\_\_\_\_ , 20\_\_\_\_ at the hour of \_\_\_\_\_\_\_ o’clock a.m / p.m.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge

{county} {courtType} Court

Executed this \_\_\_\_\_ Day of \_\_\_\_\_, 20\_\_\_\_, at the hour of \_\_\_\_\_ o’clock a.m / p.m.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Executing Officer Name and Signature