|  |  |
| --- | --- |
|  | **TELEPHONIC SEARCH WARRANT AFFIDAVIT**  **CASE NUMBER:**  **DATE:** October 4th, 2024 |

|  |  |  |
| --- | --- | --- |
| **JUDGE:** | **Hello?** | |
| **OFFICER:** | **Judge , this is** Ofc.  **of the Oro Valley Police Department. I am calling to apply for a telephonic search warrant, will you swear me in please?** | |
| **JUDGE:** | **(Judge swears you in)** | |
| **OFFICER:** | **I am calling you on (date)\_\_\_\_\_\_\_\_\_\_\_\_\_ at (time) \_\_\_\_\_\_\_\_\_\_\_\_\_\_ for the purpose of applying for a telephonic search warrant. I have just, probable, and reasonable cause to believe that:** | |
| **In the possession of:** | |  |
| **On the premises located at:** | |  |
| **In the vehicle described as:** | |  |

**There is now being possessed or concealed certain property or things described as:**

It is requested that case agents from the Oro Valley Police department, the prosecutor's office, and/or the agents thereof be granted authorization to have a computer forensic specialist make 'forensic acquisitions' of any electronic devices seized for forensic analysis. Additionally, I request that permission be granted to break codes or methods of encryption used to conceal items on said systems. After the recovery of any/all available data from the processed device(s), evidence copies of any files, records or other information deemed relevant to the investigation, as well as original acquisition files for those devices determined to contain relevant information will be retained for further proceedings.  
  
Examples of potentially relevant data which can be recovered from the seized electronic device(s) include data that may identify the owner or user of the above-described cellular communication device(s); Address books and calendars; Call histories and call logs; Audio files, and associated metadata, to include any voicemail and voice notes; Photographs and associated metadata; Video files and associate metadata; Documents and other text-based files; Text messages (SMS), multimedia messages (MMS) and their attached multimedia files, and other recorded messages, whether read or unread; Third party application data, to include usernames, passwords, account information, contacts and phonebooks, location information, correspondence, instant messages, and files; Third party applications, to include, Skype, Google Voice and other applications that can assign a second roaming telephone number; E-mail messages and attachments, whether read or unread; Internet files, to include browser history, browser cache, stored cookies, browser favorites, auto-complete form history and stored passwords; Global navigation satellite system (GNSS) data, which includes US NAVSTAR GPS and other navigation satellite systems. This data to include latitude and longitude coordinates, way points and tracks and other location data; Wireless network information, to include Service Set Identifier (SSID) and network location information; Recoverable deleted data from all above-referenced items.  
  
In some rare cases, advanced and potentially destructive data acquisition techniques such as JTAG, ISP and/or Chip-Off may be necessary to acquire the most complete data possible. In the case that such techniques are deemed necessary, justification of the techniques will be cited by the forensic specialist in their report. Once the data has been downloaded from the electronic devices, the data will be processed and examined for evidence relevant to the investigation.  
  
It is requested that case agents from the Oro Valley Police department, the prosecutor's office, and/or the agents thereof be granted authorization to have a computer forensic specialist make 'forensic acquisitions' of any electronic devices seized for forensic analysis. Additionally, I request that permission be granted to break codes or methods of encryption used to conceal items on said systems. After the recovery of any/all available data from the processed device(s), evidence copies of any files, records or other information deemed relevant to the investigation, as well as original acquisition files for those devices determined to contain relevant information will be retained for further proceedings.  
  
Examples of potentially relevant data which can be recovered from the seized electronic device(s) include data that may identify the owner or user of the above-described cellular communication device(s); Address books and calendars; Call histories and call logs; Audio files, and associated metadata, to include any voicemail and voice notes; Photographs and associated metadata; Video files and associate metadata; Documents and other text-based files; Text messages (SMS), multimedia messages (MMS) and their attached multimedia files, and other recorded messages, whether read or unread; Third party application data, to include usernames, passwords, account information, contacts and phonebooks, location information, correspondence, instant messages, and files; Third party applications, to include, Skype, Google Voice and other applications that can assign a second roaming telephone number; E-mail messages and attachments, whether read or unread; Internet files, to include browser history, browser cache, stored cookies, browser favorites, auto-complete form history and stored passwords; Global navigation satellite system (GNSS) data, which includes US NAVSTAR GPS and other navigation satellite systems. This data to include latitude and longitude coordinates, way points and tracks and other location data; Wireless network information, to include Service Set Identifier (SSID) and network location information; Recoverable deleted data from all above-referenced items.  
  
In some rare cases, advanced and potentially destructive data acquisition techniques such as JTAG, ISP and/or Chip-Off may be necessary to acquire the most complete data possible. In the case that such techniques are deemed necessary, justification of the techniques will be cited by the forensic specialist in their report. Once the data has been downloaded from the electronic devices, the data will be processed and examined for evidence relevant to the investigation.

**I, Ofc. , your affiant, am a police officer with the Oro Valley Police Department. I have been a police officer for years and have the following Training and Experience:**

The user should enter their training and experience here. Each user's TandE.txt file will be specific to themselves.

**I am investigating the crime(s) of:**

**Which I believe to have been committed on April 4th, 2024, in the county of Pima, State of Arizona.**

**Your affiant says there is probable and reasonable cause to believe that the stated property constitutes evidence which tends to show a crime has been committed and the property is subject to seizure as evidence.**

**Your affiant says that the facts in support of the issuance of this search warrant are as follows:**

|  |  |
| --- | --- |
| **Officer:** | **Based on the preceding facts, your honor, I** Ofc. **, request that a telephonic search warrant be issued.** |
| **Judge:** | **(*Await his/her reply)*** |
| **Officer:** | **I will now read verbatim to you the Standard Arizona Original Search Warrant, indicating which spaces I have completed.**  ***(Read warrant)*** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Standard Arizona Original Search Warrant**  **County of Pima, State of Arizona**   |  |  |  |  | | --- | --- | --- | --- | | **Warrant #** |  | **Date Served:** |  | | **Case #** |  | **Time Served:** |  | |

**To any peace officer in the state of Arizona:**

**Proof of affidavit having been made this date before me by Ofc. . I am satisfied that there is probable cause to believe that:**

|  |  |
| --- | --- |
| **In the possession of:** |  |
| **On the premises located at:** |  |
| **In the vehicle described as:** |  |

**In the county of Pima, state of Arizona, there is now being possessed or concealed certain property or things described as:**

It is requested that case agents from the Oro Valley Police department, the prosecutor's office, and/or the agents thereof be granted authorization to have a computer forensic specialist make 'forensic acquisitions' of any electronic devices seized for forensic analysis. Additionally, I request that permission be granted to break codes or methods of encryption used to conceal items on said systems. After the recovery of any/all available data from the processed device(s), evidence copies of any files, records or other information deemed relevant to the investigation, as well as original acquisition files for those devices determined to contain relevant information will be retained for further proceedings.  
  
Examples of potentially relevant data which can be recovered from the seized electronic device(s) include data that may identify the owner or user of the above-described cellular communication device(s); Address books and calendars; Call histories and call logs; Audio files, and associated metadata, to include any voicemail and voice notes; Photographs and associated metadata; Video files and associate metadata; Documents and other text-based files; Text messages (SMS), multimedia messages (MMS) and their attached multimedia files, and other recorded messages, whether read or unread; Third party application data, to include usernames, passwords, account information, contacts and phonebooks, location information, correspondence, instant messages, and files; Third party applications, to include, Skype, Google Voice and other applications that can assign a second roaming telephone number; E-mail messages and attachments, whether read or unread; Internet files, to include browser history, browser cache, stored cookies, browser favorites, auto-complete form history and stored passwords; Global navigation satellite system (GNSS) data, which includes US NAVSTAR GPS and other navigation satellite systems. This data to include latitude and longitude coordinates, way points and tracks and other location data; Wireless network information, to include Service Set Identifier (SSID) and network location information; Recoverable deleted data from all above-referenced items.  
  
In some rare cases, advanced and potentially destructive data acquisition techniques such as JTAG, ISP and/or Chip-Off may be necessary to acquire the most complete data possible. In the case that such techniques are deemed necessary, justification of the techniques will be cited by the forensic specialist in their report. Once the data has been downloaded from the electronic devices, the data will be processed and examined for evidence relevant to the investigation.  
  
It is requested that case agents from the Oro Valley Police department, the prosecutor's office, and/or the agents thereof be granted authorization to have a computer forensic specialist make 'forensic acquisitions' of any electronic devices seized for forensic analysis. Additionally, I request that permission be granted to break codes or methods of encryption used to conceal items on said systems. After the recovery of any/all available data from the processed device(s), evidence copies of any files, records or other information deemed relevant to the investigation, as well as original acquisition files for those devices determined to contain relevant information will be retained for further proceedings.  
  
Examples of potentially relevant data which can be recovered from the seized electronic device(s) include data that may identify the owner or user of the above-described cellular communication device(s); Address books and calendars; Call histories and call logs; Audio files, and associated metadata, to include any voicemail and voice notes; Photographs and associated metadata; Video files and associate metadata; Documents and other text-based files; Text messages (SMS), multimedia messages (MMS) and their attached multimedia files, and other recorded messages, whether read or unread; Third party application data, to include usernames, passwords, account information, contacts and phonebooks, location information, correspondence, instant messages, and files; Third party applications, to include, Skype, Google Voice and other applications that can assign a second roaming telephone number; E-mail messages and attachments, whether read or unread; Internet files, to include browser history, browser cache, stored cookies, browser favorites, auto-complete form history and stored passwords; Global navigation satellite system (GNSS) data, which includes US NAVSTAR GPS and other navigation satellite systems. This data to include latitude and longitude coordinates, way points and tracks and other location data; Wireless network information, to include Service Set Identifier (SSID) and network location information; Recoverable deleted data from all above-referenced items.  
  
In some rare cases, advanced and potentially destructive data acquisition techniques such as JTAG, ISP and/or Chip-Off may be necessary to acquire the most complete data possible. In the case that such techniques are deemed necessary, justification of the techniques will be cited by the forensic specialist in their report. Once the data has been downloaded from the electronic devices, the data will be processed and examined for evidence relevant to the investigation.

**Which property or things:**

Were stolen or embezzled  
  
Were stolen or embezzled

**Together with other fruits, instrumentalities, and evidence of the crime(s) of:**

**Which offense(s) occurred on April 4th, 2024, in the county of Pima, state of Arizona.**

**You are therefore commanded:**

**To make a search of the person(s), premises, and/or vehicle(s) listed for the property listed, and if you find the same or any part thereof, to retain such in your custody or in the custody of the agency you represent, as provided by ARS 13-3920.**

**Return this warrant to me within three (3) court business days after execution, as directed by A.R.S. Section 13-3918.**

**Given under my hand and dated this** **4th day of October, 2024.**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Ofc.**  **Oro Valley Police Department** |  | **Judge**  **court** |
|  |  | **Date:** |
|  |  | **Time:** |
|  |  |  |