
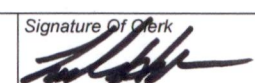


File No. 299W06 0042		STATE OF NORTH CAROLINA			
SEARCH WARRANT		<u>WAKE</u> County		In The General Court Of Justice District/Superior Court Division	
IN THE MATTER OF		<p>To any officer with authority and jurisdiction to conduct the search authorized by this Search Warrant:</p> <p>I, the undersigned, find that there is probable cause to believe that the property and person described in the application on the reverse side and related to the commission of a crime is located as described in the application.</p> <p>You are commanded to search the premises, vehicle, person and other place or item described in the application for the property and person in question. If the property and/or person are found, make the seizure and keep the property subject to Court Order and process the person according to law.</p> <p>You are directed to execute this Search Warrant within forty-eight (48) hours from the time indicated on this Warrant and make due return to the Clerk of the Issuing Court.</p> <p>This Search Warrant is issued upon information furnished under oath or affirmation by the person(s) shown.</p>			
All Content and Other Information Associated with the IMEI: "355111141087821", Maintained at Premises Controlled by Apple, Inc.					
Name Of Applicant SA M. T. Holcomb; NCSBI Name Of Additional Affiant(s) 					
RETURN OF SERVICE					
I certify that this Search Warrant was received and executed as follows:					
Date Received 03/18/25	Time Received 1:24 <input type="checkbox"/> AM <input checked="" type="checkbox"/> PM				
Date Executed 03/18/25	Time Received 1:28 <input type="checkbox"/> AM <input checked="" type="checkbox"/> PM	1:15 pm			
<input checked="" type="checkbox"/> I made a search of All content and other information associated with the IMEI: "355111141087821" maintained at premises controlled by Apple, Inc. as commanded. <input checked="" type="checkbox"/> I seized the items listed on the attached inventory. <input type="checkbox"/> I did not seize any items. <input type="checkbox"/> This Warrant WAS NOT executed within forty-eight (48) hours of the date and time of issuance and I hereby return it not executed.		Date Issued 3/18/2025	Time Issued <input type="checkbox"/> AM <input type="checkbox"/> PM	Name (type or print) Craig Croom	Signature 
		<input type="checkbox"/> Deputy CSC <input type="checkbox"/> Assistant CSC <input type="checkbox"/> CSC <input type="checkbox"/> Magistrate <input type="checkbox"/> District Ct. Judge <input checked="" type="checkbox"/> Superior Ct. Judge			
		NOTE: When issuing a search warrant, the issuing official must retain a copy of the warrant and warrant application and must promptly file them with the clerk. G.S. 15A-245(b).			
		This Search Warrant was delivered to me on the date and at the time shown below when the Office of the Clerk of Superior Court is closed for the transaction of business. By signing below, I certify that I will deliver this Search Warrant to the Office of the Clerk of Superior Court as soon as possible on the Clerk's next business day.			
Name Of Officer Making Return (type or print) SA M. T. Holcomb		Date	Time <input type="checkbox"/> AM <input type="checkbox"/> PM	Name Of Magistrate (type or print)	Signature Of Magistrate
Signature Of Officer Making Return M. T. Holcomb		This Search Warrant was returned to the undersigned clerk on the date and time shown below.			
Department Or Agency Of Officer NCSBI	Incident Number 2024-03663	Date 5/1/25	Time 1:28 <input type="checkbox"/> AM <input checked="" type="checkbox"/> PM	Name Of Clerk (type or print) Leah Hedden	Signature Of Clerk 
		<input checked="" type="checkbox"/> Dep. CSC <input type="checkbox"/> Asst. CSC <input type="checkbox"/> CSC			

APPLICATION FOR SEARCH WARRANT

I, SA M. T. Holcomb; NCSBI

(Insert name and address; or if law enforcement officer, name, rank and agency)

being duly sworn, request that the Court issue a warrant to search the person, place, vehicle, and other items described in this application and to find and seize the property and person described in this application. There is probable cause to believe that *(Describe property to be seized; or if search warrant is to be used for searching a place to serve an arrest warrant or other process, name person to be arrested)*

SEE ATTACHED "PROPERTY/EVIDENCE TO BE SEIZED"

constitutes evidence of a crime and the identity of a person participating in a crime, *(Name crime)* N.C.G.S. 4-(a); Obstruction of Justice

and is located *(Check appropriate box(es) and fill in specified information)*

- ☒ in the following premises *(Give address and, if useful, describe premises)*
SEE ATTACHED "PLACES TO BE SEARCHED"

(and)

- ☒ on the following person(s) *(Give name(s) and, if useful, describe person(s))*
SEE ATTACHED "PLACES TO BE SEARCHED"

(and)

- ☒ in the following vehicle(s) *(Describe vehicle(s))*
SEE ATTACHED "PLACES TO BE SEARCHED"

(and)

- ☒ *(Name and/or describe other places or items to be searched, if applicable)*
SEE ATTACHED "PLACES TO BE SEARCHED"

The applicant swears or affirms to the following facts to establish probable cause for the issuance of a search warrant:

SEE ATTACHED "PROBABLE CAUSE AFFIDAVIT".

SWORN/AFFIRMED AND SUBSCRIBED TO BEFORE ME

Date

03/18/2024

Date

3/18/2025

Name Of Applicant (type or print)

SA M. T. Holcomb

Signature

Signature Of Applicant

Matthew Holcomb

☐ Magistrate

☐ Dep. CSC

☐ Asst. CSC

☐ Clerk Of Superior Court

☒ Judge

- ☒ In addition to the affidavit included above, this application is supported by additional affidavits, attached, made by SA M. T. Holcomb; NCSBI

- ☐ In addition to the affidavit included above, this application is supported by sworn testimony, given by _____

This testimony has been *(check appropriate box)* ☐ reduced to writing
☐ recorded, and I have filed any such writing/recording with the clerk.

NOTE: If more space is needed for any section, continue the statement on an attached sheet of paper with a notation saying "see attachment." Date the continuation and include on it the signatures of applicant and issuing official.

IN THE MATTER OF:

ATTACHMENT TO APPLICATION
FOR SEARCH WARRANT

All Content and Other Information Associated with
the IMEI: "355111141087821",
Maintained at Premises Controlled by Apple, Inc.

ATTACHMENT I- PROPERTY/EVIDENCE TO BE SEIZED:

The facts and circumstances outlined in this affidavit suggest that there is cause to believe evidence of the commission of the crime of Obstruction of Justice, a violation of North Carolina General Statute 4-(a), may be found in the above-mentioned Apple, Inc. accounts (hereinafter "the Accounts"). To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed. The following material is sought for the time period of **October 6, 2024 to January 30, 2025** and extending ten (10) days from the date of issuance as signed by the Court including, but not limited to:

- All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");
- The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

Matthew Holcomb
Signature of Applicant

☐ Deputy CSC ☐ Ass. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.

- The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- All records pertaining to the types of service used;
- All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).
- The Provider is hereby ordered to disclose the above information to the government within **March 31, 2025** of service of this warrant.

ATTACHMENT II- PLACES TO BE SEARCHED:

SWORN TO AND SUBSCRIBED BEFORE ME

THIS 18th DAY OF March, 20 25.

Matthew Holcomb

Signature of Applicant

☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

IN THE MATTER OF:

ATTACHMENT TO APPLICATION
FOR SEARCH WARRANT

**All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.**

This warrant is directed to Apple, Inc. (the "Provider"), a company headquartered at 1 Infinite Loop, Cupertino, CA, and applies to all content and other information within the Provider's possession, custody, or control associated with the **IMEI: "355111141087821"** (hereafter the "Subject Account"). This legal process demands that Apple provide the requested records even if maintained on offshore servers outside of the United States.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in ATTACHMENT I.

Upon receipt of the production, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of North Carolina General Statute 4-(a), Obstruction of Justice, which may be contained within the furnished records.

ATTACHMENT III- PROBABLE CAUSE AFFIDAVIT:

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

Matthew Holcomb

Signature of Applicant

IN THE MATTER OF:

ATTACHMENT TO APPLICATION
FOR SEARCH WARRANT

**All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.**

The Affiant swears to the following facts to establish probable cause for the issuance of a search warrant:

The Affiant swears to the following facts to establish probable cause for the issuance of a search warrant:

I, SA M.T. Holcomb, hereby swear and affirm that the following affidavit is based upon my personal knowledge, training, and experience as a sworn law enforcement officer and upon factual information which I have received from other persons as hereinafter described.

I, Special Agent M. T. Holcomb, being duly sworn hereby swear and affirm, am a sworn Special Agent employed with the North Carolina State Bureau of Investigation, hereafter referred to as NCSBI. I have received a Bachelor of Science Degree in Criminal Justice with a concentration in Strategic Intelligence from Liberty University in 2021. After college, I attended and graduated from Basic Law Enforcement Training at Alamance Community College in August of 2021. I have received more than 650 hours of training in Basic Law Enforcement Training which included courses in: Elements of Crime, Search and Seizure Law, Criminal Investigations, and Controlled Substances.

In July of 2022, I joined the Burlington Police Department where I served as a Police Officer prior to becoming employed with the NCSBI in December 2022. I have received advanced training in investigations in the 54th NC SBI's 12-week Special Agent Academy in 2023. During the Special Agent Academy, I received 80 hours of training from Police Law Institute focusing on arrest, search, seizure and constitutional rights in North Carolina.

I have investigated homicides, officer involved shootings, death in custody's, public corruption, drug trafficking, sexual assaults, and missing persons investigations throughout my career with the NCSBI. In addition, with my time with the NCSBI, I have conducted and assisted in the preparation and execution of numerous search warrants and assisted with the apprehension of violent criminals.

The information received during the course of this investigation is discussed in this affidavit and is believed to be true and accurate by SA M. T. Holcomb.

On January 15, 2025, District Attorney L. Freeman with the 10th Prosecutorial District requested assistance from the North Carolina State Bureau of Investigation with investigating the circumstances surrounding a traffic accident that occurred on October 7, 2024, in Raleigh, North Carolina. It was reported that Trooper Garret Macario of the North Carolina State Highway Patrol provided false information to a Raleigh Police Officer who was conducting a traffic accident investigation.

Trooper Macario's body worn camera video footage of the incident was provided to SA Holcomb by Captain C. Parks with the NCSHP on January 16, 2025.

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

Matthew Holcomb

Signature of Applicant

☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

Page 4 of 9

IN THE MATTER OF:

ATTACHMENT TO APPLICATION
FOR SEARCH WARRANT

**All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.**

The following was observed by SA Holcomb while reviewing Trooper Macario's body worn camera.

On October 7, 2024, at approximately 2:30 a.m. Trooper Macario with the NCSHP was conducting traffic enforcement in the area of Capital Boulevard and Wake Forest Road in Raleigh, North Carolina. Trooper Macario attempted a traffic stop on a citizen, Tyrone Mason B/M/DOB: 07/28/1993 for a movement violation, but disengaged based on the circumstances of Mason's driving behaviors. After Trooper Macario was disengaged, Mason's vehicle wrecked near the median of the roadway. Mason ultimately died from his wounds from the traffic accident. After the wreck, Trooper Macario parked his vehicle in the area where Mason's vehicle was wrecked. Trooper Macario contacted NCSHP Troop C, District 3, on the radio and requested the Raleigh Police Department and Fire and EMS to respond to the wreck.

While on scene, at approximately 2:32 a.m., Trooper Macario's body worn camera shows him making a phone call to Sergeant Matthew Morrison with the NCSHP. Trooper Macario explained to Sgt. Morrison the incident that just took place. Sgt. Morrison asked Trooper Macario if he called in a 10-43, Vehicle Chase over the radio. Trooper Macario told Sgt. Morrison he did not call 10-43, Vehicle Chase. Sgt. Morrison told Trooper Macario that the traffic accident was RPD's problem. Sgt. Morrison then told Trooper Macario not to tell responding Raleigh Police Department Officers that he tried to stop Mason before the traffic accident.

Officer R. Urena with RPD asked Trooper Macario if he was pulling over Mason which lead to the traffic accident. Trooper Macario told Officer Urena that he was not trying to pull Mason over and that he came up on the wreck and saw the smoke and debris from the vehicle.

Trooper Macario's body worn camera footage lasted approximately 11 minutes and 45 seconds.

On January 15, 2025, Captain C. Parks with the NCSHP provided SA Holcomb with Trooper Macario's personal cellular telephone number which was 919-815-9142. Trooper Macario did not have a work phone. Captain Parks also provided Sgt. Morrison's personal cellular telephone number, which was 704-575-8064 and his work cellular telephone number which was 919-971-5416. Sgt. Morrison's work cellular telephone number was issued by NCSHP to communicate with other subordinates within the agency.

On January 24, 2025, SA Holcomb executed a search warrant to Verizon Wireless for Cellular Telephone number 919-971-5416. Verizon provided subscriber information that listed Matthew Morrison's name on the account. Verizon also included device information which listed the cellphone as an Apple Midnight iPhone 14 and the IMEI: "355111141087821".

Based on the above information, this affiant believes that information received as a result of this search warrant will disclose communications between Trooper Macario and Sgt. Morrison in reference to conversations had regarding the traffic accident Mason was involved in.

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

Matthew Holcomb

Signature of Applicant

☐ Deputy CSC ☐ Asst. CSC ☒ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

IN THE MATTER OF:

ATTACHMENT TO APPLICATION
FOR SEARCH WARRANT

**All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.**

Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

Matthew Holcomb

Signature of Applicant

IN THE MATTER OF:

ATTACHMENT TO APPLICATION
FOR SEARCH WARRANT

**All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.**

Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

Matthew Holcomb
Signature of Applicant

IN THE MATTER OF:

ATTACHMENT TO APPLICATION
FOR SEARCH WARRANT

**All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.**

use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

In this affiant's training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

Matthew Holcomb

Signature of Applicant

☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge

Page 8 of 9

**All Content and Other Information Associated with
the "355111141087821",
Maintained at Premises Controlled by Apple, Inc.**

In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

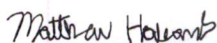
Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

The applicant would respectfully request the court issue a search warrant for the material outlined in ATTACHMENT I of the above-mentioned Apple, Inc. account.

All information and facts provided in this affidavit are true and accurate to the best of the applicant's knowledge. The applicant feels that there is sufficient probable cause for the issuance of a search warrant for the evidence, fruits, and instrumentalities of violations of North Carolina General Statute 4-(a), Obstruction of Justice which may be contained within the furnished records

SWORN TO AND SUBSCRIBED BEFORE ME
THIS 18th DAY OF March, 20 25.

 
☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☒ Judge



Signature of Applicant

IN THE MATTER OF:
APPLICATION

All Content and Other Information Associated with
the IMEI: "35521114108782",
Maintained at Premises Controlled by Apple, Inc.

ATTACHMENT TO
FOR SEARCH WARRANT

SWORN TO AND SUBSCRIBED BEFORE ME
THIS _____ DAY OF _____, 20_____.

☐ Deputy CSC ☐ Asst. CSC ☐ Clerk of Sup. Ct. ☐ Mag. ☐ Judge

Matthew Halverson
Signature of Applicant

Page 10 of 1

STATE OF NORTH CAROLINA

File No.

WAKE

County

In The General Court Of Justice

☒ District ☒ Superior Court Division

IN THE MATTER OF:

Name

All Content and Other Information Associated with the
IMEI: "355111141087821", Maintained at Premises
Controlled by Apple, Inc.

INVENTORY OF ITEMS SEIZED
PURSUANT TO SEARCH

G.S. 15A-223, -254, -257

I, the undersigned officer, executed a search of:

Person, Premises Or Vehicle Searched

All Content and Other Information Associated with the
IMEI: "355111141087821", Maintained at Premises
Controlled by Apple, Inc.

Date Of Search

03/21/2025

This search was made pursuant to

- ☒ 1. a search warrant issued by: Superior Court Judge C. Croom
- ☐ 2. consent to search given by: _____
- ☐ 3. other legal justification for the search: _____

The following items were seized:

- Data Files

Original - File

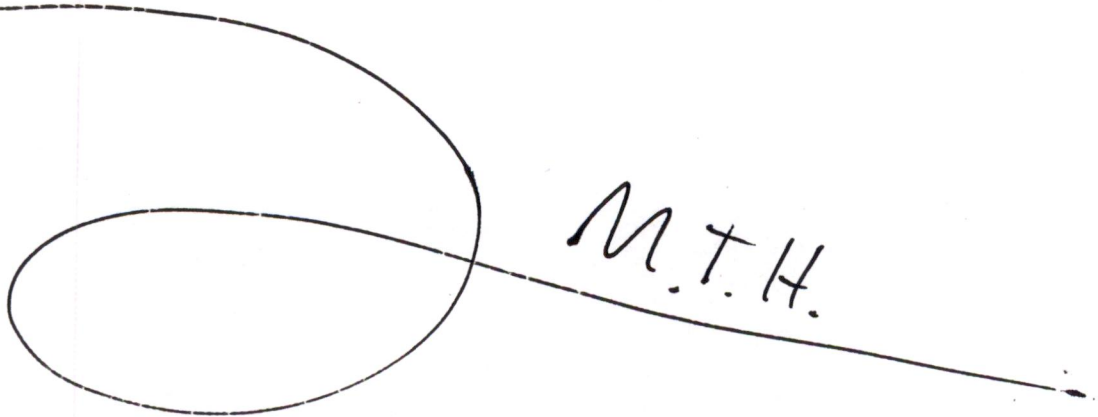
Copy - For Search by Warrant of a Person, to Person from Whom Items Taken

Copy - For Search by Warrant of Vehicle/Premises, to Owner or Person in Apparent Control; if No Such Person Present, Leave Copy Affixed Thereon

Copies - For Search by Consent, to Person Giving Consent and Owner of Vehicle/Premises Searched, if Known

(Over)

Items Seized Continued:

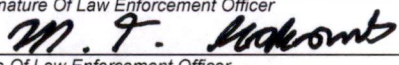
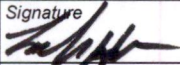


- ☐ 1. I left a copy of this inventory with the person named below, who is:
- ☐ a. the owner of the premises searched.
 - ☐ b. the owner of the vehicle searched.
 - ☐ c. the person in apparent control of the premises searched.
 - ☐ d. the person in apparent control of the vehicle searched.
 - ☐ e. the person from whom the items were taken.

- ☒ 2. As no person was present, I left a copy of this inventory:
- ☒ a. in the premises searched, identified on the reverse.
 - ☐ b. in the vehicle searched, identified on the reverse.

Name And Address Of Person To Whom A Copy Of This Inventory Was Delivered, If Any
Apple, inc.

The law enforcement agency identified below will hold the seized property subject to court order.

SWORN/AFFIRMED AND SUBSCRIBED TO BEFORE ME		Name Of Law Enforcement Officer (type or print) SA M. T. Holcomb
Date 5/1/25	Name (type or print) Leah Hedden	Signature Of Law Enforcement Officer 
<input type="checkbox"/> Notary	Signature 	Title Of Law Enforcement Officer Special Agent
SEAL	Date My Commission Expires	Name And Address Of Agency North Carolina State Bureau of Investigation 3320 Garner Road, Raleigh, NC 27610
	County Where Notarized	
<input checked="" type="checkbox"/> Deputy CSC <input type="checkbox"/> Assistant CSC <input type="checkbox"/> Clerk Of Superior Court <input type="checkbox"/> Magistrate		

ACKNOWLEDGMENT OF RECEIPT

I, the undersigned, received a copy of this inventory.

Date	Signature Of Person Receiving Inventory
------	---