

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
ONE PREMISES AND ONE PERSON INCLUDING ANY
AND ALL DIGITAL DEVICES OWNED, USED, OR
CONTROLLED BY THAT PERSON UNDER RULE 41

Case No. 24-SW-055

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A (incorporated by reference)

Located within the jurisdiction of the District of Columbia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 641, 2 (theft of government property and aiding and abetting theft of government property);	
18 U.S.C. § 1752(a)(1) (entering or remaining in restricted buildings or grounds);	
18 U.S.C. § 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds);	
40 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings);	
40 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building).	

The application is based on these facts:

See Affidavit in Support of Application for Search Warrant.

- Continued on the attached sheet.
- Delayed notice of _____ days *(give exact ending date if more than 30 days)*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Printed name and title
Special Agent

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone _____ *(specify reliable electronic means)*.

Date: 3/13/2024

City and state: Washington, D.C.



Judge's signature

Robin M. Meriweather
(United States Magistrate Judge)

2024.03.13
13:20:29 -04'00'

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

Original

Duplicate Original

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of)
(Briefly describe the property to be searched)
(or identify the person by name and address))
ONE PREMISES AND ONE PERSON INCLUDING ANY)
AND ALL DIGITAL DEVICES OWNED, USED, OR)
CONTROLLED BY THAT PERSON UNDER RULE 41)

Case No. 24-SW-055

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located within the jurisdiction of the District of Columbia.

(identify the person or describe the property to be searched and give its location):

See Attachment A (incorporated by reference).

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B (incorporated by reference).

YOU ARE COMMANDED to execute this warrant on or before March 26, 2024 (not to exceed 14 days)
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.



Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Robin M. Meriweather
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for days (not to exceed 30) until, the facts justifying, the later specific date of 2024.03.13

Date and time issued: 3/13/2024



2024.03.13
13:21:18 -04'00'
Judge's signature

City and state: Washington, D.C.

Robin M. Meriweather
United States Magistrate Judge

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.: 24-SW-055	Date and time warrant executed:	Copy of warrant and inventory left with:
------------------------	---------------------------------	------------------------------------------

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

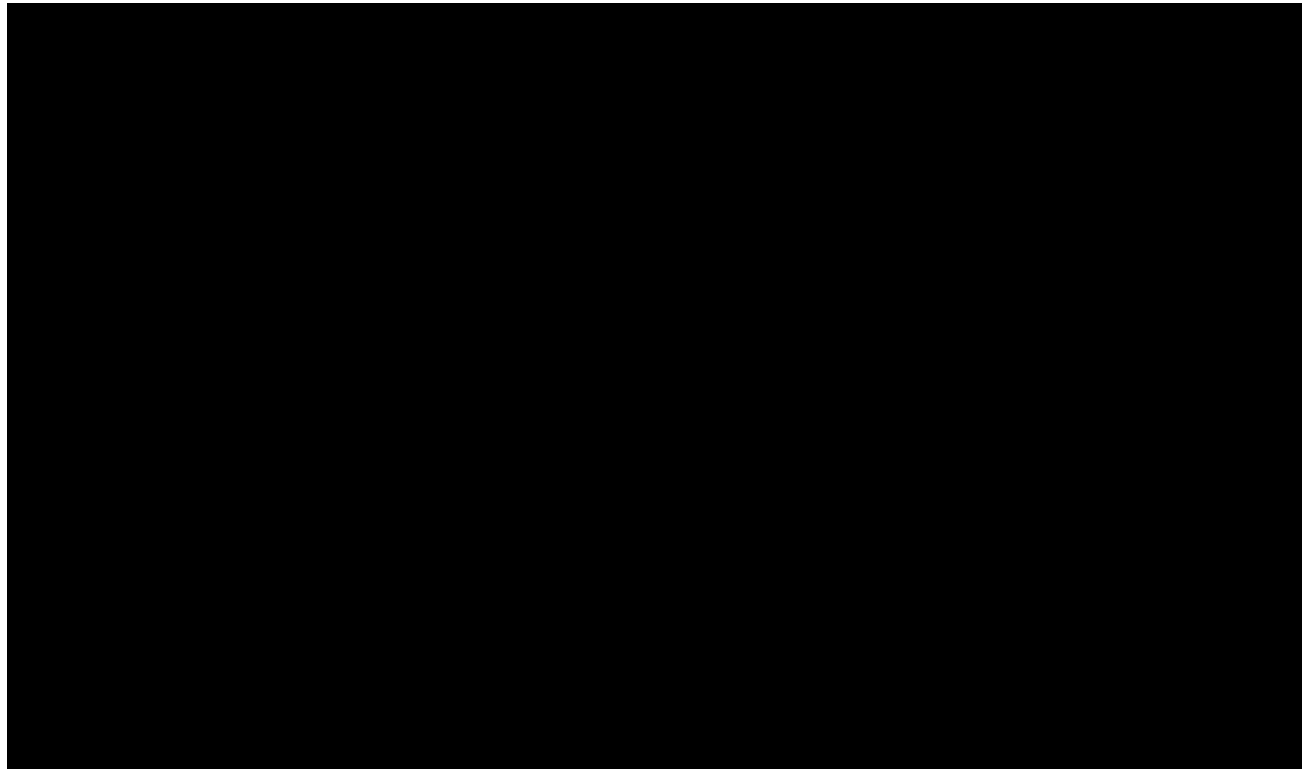
Executing officer's signature

Printed name and title

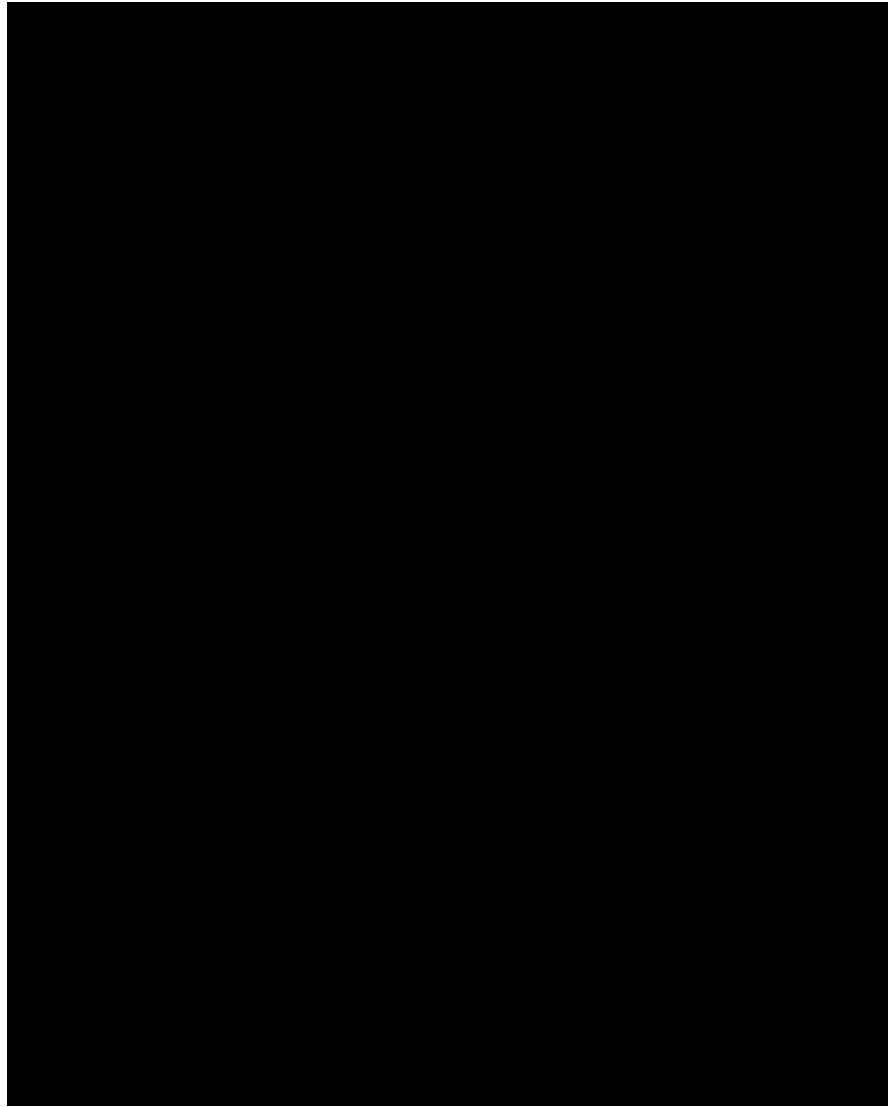
ATTACHMENT A-1

Property to be searched

The property to be searched is [REDACTED] (“PREMISES”), further described as a multi-story apartment building with a modern glass façade, located across from the center field entrance to Nationals Park. The PREMISES is located on the fifth floor of the building and the numbers “[REDACTED]” appear to the left of the door. The PREMISES contains two bedrooms and one bathroom. On December 5, 2023, the Federal Bureau of Investigation interviewed employees of the apartment building who provided records confirming that ISABELLA MARIA DELUCA rents [REDACTED] with a roommate and that the lease is current through April 27, 2024.



View of Property looking North at intersection of Half Street SE and N Street SE



Entrance to [REDACTED]



Entrance to [redacted]



Floor Plan for [REDACTED]

ATTACHMENT A-2

Person to be searched

The person to be searched is ISABELLA MARIA DELUCA (“DELUCA”) (DOB: [REDACTED]) (SSN: [REDACTED]), as pictured below, provided that such person is located within the District of Columbia.



This warrant further authorizes the search and forensic examination pursuant to Attachment B of any cellular phone or digital device seized from the person of DELUCA for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. §§ 641, 2 (theft of government property and aiding and abetting theft of government property), 18 U.S.C. § 1752(a)(1) (entering or remaining in restricted buildings or grounds), 18 U.S.C. § 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds), 40 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings) and 40 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building) (the “TARGET OFFENSES”) (the “TARGET OFFENSES”) that have been committed by ISABELLA MARIA DELUCA (“the Subject”) and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to:

- a. Evidence of the TARGET OFFENSES, including but not limited to: emails, text messages, direct messages, social media posts, communications, photographs, videos, and other writings from November 3, 2020 to March 31, 2021;
- b. Evidence of any conspiracy, planning, or preparation to commit those offenses;
- c. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
- d. Evidence concerning materials, devices, or tools that were used to unlawfully commit the TARGET OFFENSES;
- e. Evidence of communication devices used in relation to the TARGET OFFENSES;
- f. Evidence of the state of mind of the subject and/or other co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
- g. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters

relating to the criminal activity under investigation, including records that help reveal their whereabouts.

- h. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
 - i. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
 - j. Evidence concerning the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
 - k. Evidence concerning efforts to obstruct, impede, or disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
 - l. Evidence concerning the breach and unlawful entry of the United States Capitol on January 6, 2021;
 - m. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;
 - n. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;
 - o. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;
 - p. Evidence concerning awareness that the U.S. Capitol was closed to the public on January 6, 2021;
 - q. Evidence of DELUCA's presence at the U.S. Capitol on or around January 6, 2021;
 - r. Evidence concerning the results of, challenges to, or questions about the legitimacy of the 2020 Presidential Election;
 - s. Evidence regarding the riot at the U.S. Capitol on January 6, 2021;
 - t. Clothing and other items that reflect evidence of DELUCA's presence at the U.S. Capitol on January 6, 2021.
2. Records and information that constitute evidence of identity, including but not

limited to:

- a. clothing worn by DELUCA on January 6, 2021, to include a brown sweater and a red, white, and blue neck gaiter.
 - b. Clothing, paraphernalia, and other articles that reflect evidence of having participated in the unlawful activity at the U.S. Capitol, including evidence of pepper spray or other non-lethal crowd control remnants;
3. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:
 - a. Any records and/or evidence revealing DELUCA’s presence at the January 6, 2021, riot;
 - b. DELUCA’s (and others’) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
 - c. DELUCA’s (and others’) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021.
4. Photographs, in particular photographs of DELUCA, other rioters, co-conspirators, or events in Washington D.C. on January 6, 2021, which constitute evidence of the TARGET OFFENSES.
5. Cellular telephones, SIM cards, computers, laptops, I-Pads, DVDs, hard drives, and electronic storage devices, and receipts reflecting their ownership and use, which contain records or evidence of the commission of the TARGET OFFENSES; and
6. Digital devices used in the commission of, or to facilitate, the above-described TARGET OFFENSES.
7. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities relevant to commission of the TARGET OFFENSES as described in the search warrant affidavit and above, hereinafter the “Device(s)”:

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
- e. evidence of the times the Device(s) was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
- g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
- h. records of or information about Internet Protocol addresses used by the Device(s);
- i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

During the execution of the search described in Attachments A-1 and A-2, law enforcement personnel are also specifically authorized to obtain from DELUCA (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that DELUCA's physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) any of the Device(s) found at the PREMISES,
- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the DELUCA state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access

the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel DELUCA to state or otherwise provide that information. However, the voluntary disclosure of such information by DELUCA is permitted. To avoid confusion on that point, if agents in executing the warrant ask DELUCA for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires DELUCA to provide such information, and will make clear that providing any such information is voluntary and that DELUCA is free to refuse the request.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “digital devices” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog

tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF:
ONE PREMISES AND ONE PERSON
INCLUDING ANY AND ALL DIGITAL
DEVICES OWNED, USED, OR
CONTROLLED BY THAT PERSON
UNDER RULE 41

SW No. 24-SW-055

UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE

I, [REDACTED], being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [REDACTED], and the person of ISABELLA MARIA DELUCA (“DELUCA”), including any and all digital devices owned, used, or controlled by DELUCA, hereinafter collectively the “PREMISES,” further described in Attachments A-1 and A-2, for the things described in Attachment B.

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement. Wherever in this affidavit I quote statements, those quotations have been taken from draft transcripts, which are subject to further revision.

3. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I have drawn from my training, experience, and knowledge of the investigation.

AFFIANT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) assigned to [REDACTED]. I have been in this position for more than seven years. During that time, I have investigated criminal cases relating to international terrorism, domestic terrorism, bomb threats, civil disturbances, and riots. In addition to my on-the-job experience, the FBI has provided me with extensive training in domestic terrorism and the techniques used to investigate allegations of domestic terrorism. As such, I am an “investigative or law enforcement officer” of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code, including the TARGET OFFENSES defined below.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 641, 2 (theft of government property and aiding and abetting theft of government property); 18 U.S.C. § 1752(a)(1) (entering or remaining in restricted buildings or grounds); 18 U.S.C. § 1752(a)(2)

(disorderly and disruptive conduct in a restricted building or grounds); 40 U.S.C. § 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings); and 40 U.S.C. § 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building) (the “TARGET OFFENSES”) that have been committed by DELUCA and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, DELUCA, as well as others observed by DELUCA. There is also probable cause to search the PREMISES, further described in Attachment A-1, and DELUCA, further described in Attachment A-2, for the things described in Attachment B.

PROBABLE CAUSE

Background – The U.S. Capitol on January 6, 2021

6. U.S. Capitol Police (“USCP”), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

7. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate

side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. The entirety of this area was barricaded and off limits to the public on January 6, 2021.

8. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside of the U.S. Capitol.

9. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

10. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 ("Certification"). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m. EST, the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

11. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

12. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

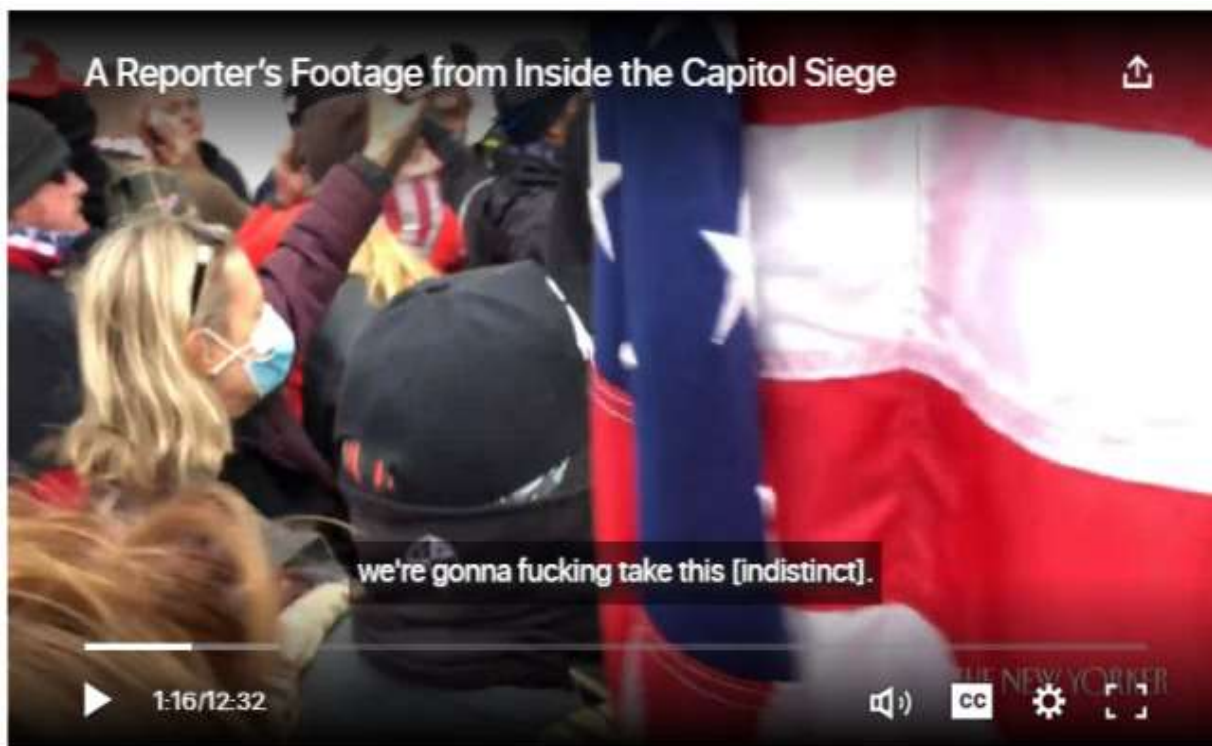
13. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

14. Media reporting showed a group of individuals outside of the Capitol chanting, “Hang Mike Pence.” I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

15. At approximately 2:00 p.m. EST, some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by USCP officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

16. Beginning shortly after 2:00 p.m. EST, individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows

an unknown individual saying to a crowd outside the Capitol building, “We’re gonna fucking take this,” which your affiant believes was a reference to “taking” the U.S. Capitol.



17. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine.

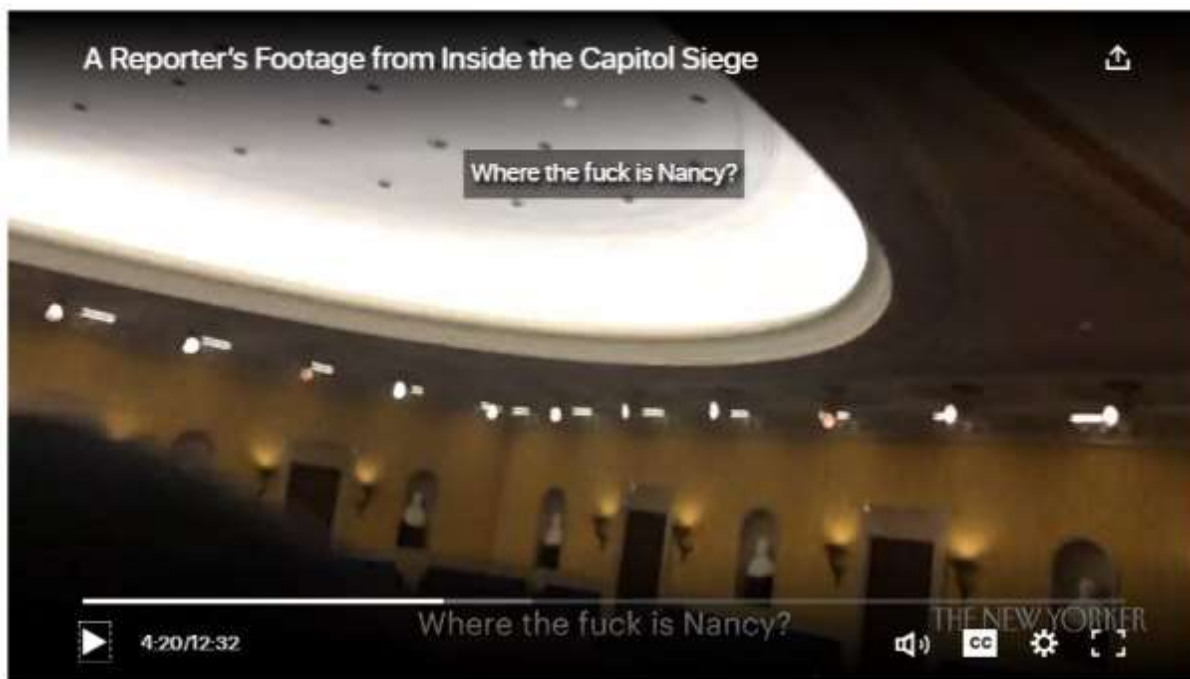
18. Between approximately 2:10 p.m. EST and 2:30 p.m. EST, Vice President Pence evacuated the Senate Chamber, and the Senate and House of Representatives were locked down and went into recess. Both the Senate and the House of Representatives Chamber were evacuated.

19. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

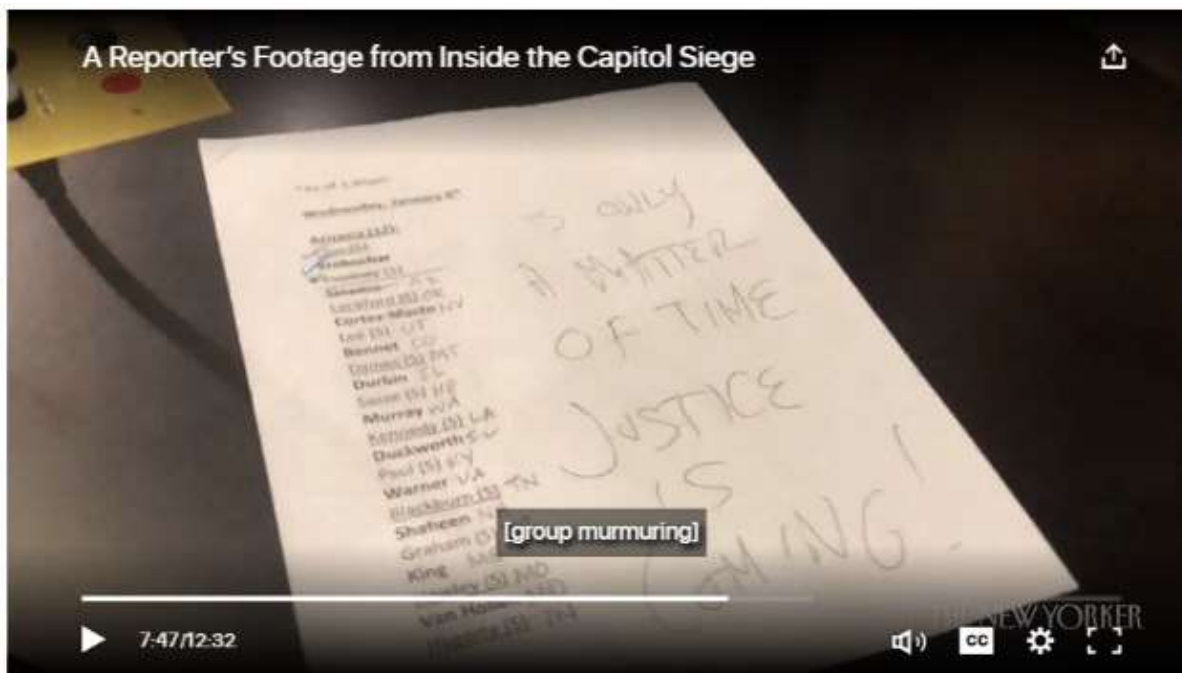
20. At around 2:47 p.m. EST, subjects broke into the Senate Chamber not long after it had been evacuated. Publicly available video shows an individual asking, “Where are they?” as they opened up the door to the Senate Chamber. Based upon the context, I believe that the word “they” is in reference to members of Congress.



21. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments and the context, I believe that the “Nancy” being referenced was the then-Speaker of the House of Representatives, Nancy Pelosi.



22. One subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated “A Matter of Time Justice is Coming.”



23. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals are expected to be taken into custody.



24. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

25. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. EST.

26. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

27. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

28. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. EST the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the U.S. Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

29. Beginning around 8:00 p.m. EST, the Senate resumed work on the Certification.

30. Beginning around 9:00 p.m. EST, the House resumed work on the Certification.

31. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3:00 a.m. EST on January 7, 2021.

32. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of

violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

33. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in and around the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

34. Many subjects on news footage in the area of the U.S. Capitol are seen using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above, as well as statements about these activities.

35. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:



1

¹ *Congresswoman: Capitol Building Takeover An 'Attempted Coup,'* CBS Los Angeles (Jan. 6, 2021), <https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/>



2

² <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>.



3

Facts Specific to This Application

Background

36. On January 9, 2021, the FBI received an online tip identifying DELUCA as a possible suspect who participated in the January 6, 2021 riot at the U.S. Capitol. The tipster alleged that DELUCA deleted social media posts about being at the U.S. Capitol on January 6.

37. After receiving the tip, the FBI telephonically interviewed DELUCA on January 21, 2021. DELUCA admitted to the FBI that she was present at the U.S. Capitol on January 6, 2021, but she claimed that she never entered the U.S. Capitol building. DELUCA further explained

³ *Arkansas Man Admits to Storming Capitol, Sitting at Nancy Pelosi's Desk*, THV 11 (Jan. 7, 2021), <https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e>.

that she went to the U.S. Capitol with some friends, but they were eventually separated from each other.

38. The FBI also telephonically interviewed DELUCA's mother on January 21, 2021. According to DELUCA's mother, DELUCA went to the U.S. Capitol with some friends, but DELUCA did not go inside the U.S. Capitol building. DELUCA's mother further stated that she viewed DELUCA's live feed Instagram video and saw DELUCA standing outside the U.S. Capitol.

39. Based on the above, the FBI opened an investigation of DELUCA. According to subpoenaed bank records, DELUCA made several purchases in the Washington D.C. area between January 5, 2021 and January 8, 2021. On January 5, 2021, DELUCA incurred a \$108.00 charge from Amtrak that noted "Orig: NYP, Dest: WAS." These codes indicate her trip originated at New York Penn Station in New York, New York, and her destination was Union Station in Washington, D.C. Records subpoenaed from Amtrak confirmed that DELUCA traveled from New York City to Washington, D.C. on January 5.

40. On January 6, 2021, DELUCA incurred a charge of \$160.86 from the Kimpton Lorien Hotel, which is located at 1600 King Street, Alexandria, Virginia. Records subpoenaed from the Kimpton Lorien Hotel confirmed that DELUCA checked in on January 6, 2021 and checked out on January 8, 2021. On January 6, 2021, DELUCA also incurred a charge from Dunkin Donuts Store No. 350957 located at 1101 14th Street NW in Washington, D.C., which is approximately 1.9 miles from the U.S. Capitol. She also incurred a charge from CVS Pharmacy Store No. 1334 located at 717 14th Street NW in Washington, D.C., which is approximately 1.5 miles from the U.S. Capitol.

41. During its investigation, the FBI lawfully obtained a search warrant for DELUCA's Instagram accounts on July 13, 2022. Subscriber records from Instagram indicate that the account with username isabellamdeluca is subscribed to by DELUCA. On the evening of January 5, 2021, DELUCA's Amtrak train broke down near Baltimore, Maryland. DELUCA messaged others on Instagram, "My train isn't working" and "I need a ride to dc." She also posted the following Instagram story. DELUCA's Instagram messages suggest that she eventually received a ride to Alexandria, where the Kimpton Lorien Hotel is located, in the early morning hours of January 6, 2021.



Image 1

DELUCA's Participation in the Riot at the U.S. Capitol on January 6, 2021

42. At 2:55 p.m. EST on January 6, 2021, DELUCA replied to a Twitter post saying, “Fight back or let politicians steal and election? Fight back!”⁴

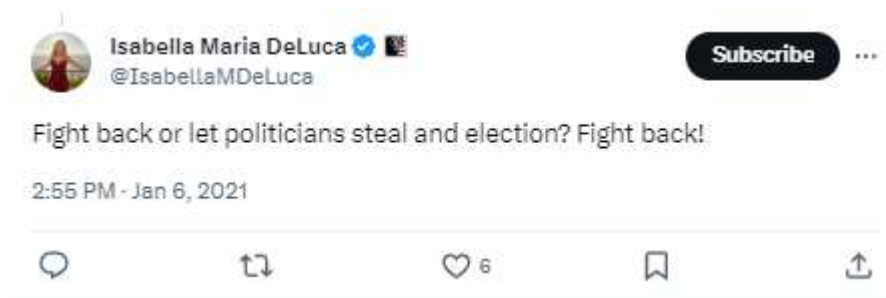


Image 2

43. Shortly thereafter, at 3:20 p.m. EST, an Instagram user messaged DELUCA, “I’m walking to the Capitol!” A few minutes later, DELUCA responded, “Okay! I’m going to head there now.” DELUCA later messaged the same person, “I’m here,” at approximately 3:46 p.m. EST.

44. Video identified from U.S. Capitol Police CCTV surveillance footage and open-source video footage place a woman matching DELUCA’s appearance inside and around the U.S. Capitol on January 6, 2021. In all photographs and videos, DELUCA is wearing a brown jacket,

⁴ The FBI also lawfully obtained a search warrant for DELUCA’s Twitter (now X) account on July 13, 2022. Subscriber records from Twitter indicate that the account with username @IsabellaMDeLuca is subscribed to by DELUCA. A further review of DELUCA’s Twitter account revealed that there were no tweets (as opposed to replies and direct messages) between January 3, 2021 and January 10, 2021.

black pants, white shoes, and at times is wearing a red, white, and blue neck gaiter partially covering her face.

45. Based on your affiant's review of video evidence, DELUCA can be seen (1) within the restricted area around the U.S. Capitol; (2) recording video and/or taking photographs within the restricted area; (3) entering Senate Terrace Room 2 Mezzanine ("ST-2M") through a broken window on the Lower West Terrace of the U.S. Capitol; and (4) removing, and aiding and abetting other rioters in removing, a table from ST-2M and passing it to rioters outside through another broken window. This table was subsequently used to assault law enforcement officers guarding the Lower West Terrace Tunnel (the "Tunnel") as described below.⁵

46. Around 4:24 p.m. EST, CCTV surveillance footage captured DELUCA, circled in yellow, within the restricted area on the temporary inaugural platform constructed on the Lower West Terrace of the U.S. Capitol, as depicted in Image 3 below. In this Image, DELUCA appeared to cover her face from tear gas blowing in the wind. She remained in this area for several minutes and appeared to be using her cell phone, as shown in Image 4 below.

⁵ The Tunnel was a corridor entryway that led into the U.S. Capitol. After the police perimeter was breached on the West Plaza of the U.S. Capitol, many law enforcement officers retreated into the Tunnel to regroup. However, rioters streamed into the Tunnel in large numbers where they began to fight the police in an attempt to enter the U.S. Capitol. A group of officers using their bodies to barricade the entrance constituted the only barrier between the rioters in the Tunnel and entry into the Capitol building. Some of the most vicious assaults on law enforcement on January 6, 2021 occurred in the area by the Tunnel.



Image 3

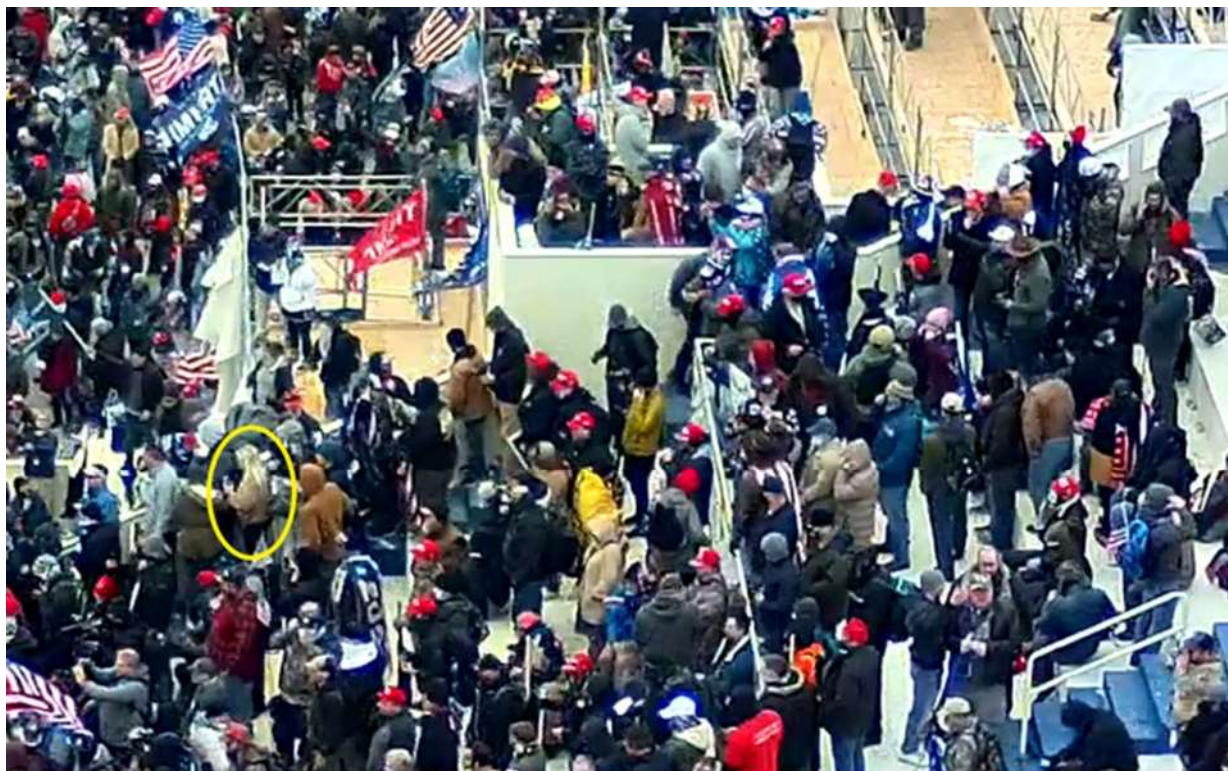


Image 4

47. From there, Deluca continued to descend the inaugural platform. Around 4:30 p.m. EST, DELUCA arrived in an area near the Tunnel and outside of ST-2M, which is directly to the left of the Tunnel (as one faces the Tunnel). Image 5 below is a screenshot from an open-source video showing DELUCA using her cell phone to record video and/or take photographs outside of ST-2M. ST-2M is one of a suite of conference rooms available for members of congress and their staffs. Although ST-2M was unoccupied on January 6, 2021, it is considered a sensitive location that is not open to members of the public.



Image 5

48. Images 6 and 7 below are also screenshots from open-source videos. DELUCA continued to record video and/or take photographs outside of ST-2M, witnessing rioters inside the room steal pieces of furniture, including a lamp and a chair, and passing them to the rioters outside.



Image 6



Image 7

49. DELUCA then entered ST-2M through one of the lower windows that had been broken by rioters, as shown in Image 8 below.



Image 8

50. Approximately 90 seconds after entering ST-2M, DELUCA passed, and assisted other rioters in passing, a table out of one of the broken windows, as depicted in Image 9 below.



Image 9

51. After DELUCA passed the table out of the window, DELUCA appeared to use her cell phone to record video and/or take photographs of the scene, as shown in Image 10 below. At the same time, rioters passed the table in the direction of the Tunnel, where it was subsequently used as a weapon against law enforcement officers.



Image 10

52. About two-and-a-half minutes after entering, DELUCA exited ST-2M through the same broken window through which she passed the table, as depicted in Image 11 below. As DELUCA was climbing out of the window, the rioter dressed in all black with a neck tattoo used a baseball bat to smash the adjacent window. During her exit, DELUCA appeared to drop her cell phone and another rioter picked it up and passed it to her, as shown in Image 12 below.



Image 11



Image 12

53. While inside ST-2M, DELUCA witnessed a chaotic scene with overturned and broken furniture thrown about the room haphazardly. Image 13 below is a screenshot from a cell phone video taken inside ST-2M around the same time DELUCA was there. Later in the same video, DELUCA can be seen standing on the ledge outside the ST-2M windows.



Image 13

54. Image 14 is a screenshot from an open-source video. DELUCA, with the neck gaiter partially covering her face, remained on the ledge outside ST-2M for approximately the next two minutes. At one point, DELUCA appeared to be observing the chaos at the mouth of the Tunnel, including the rioters passing a long wooden beam towards the mouth of the Tunnel, as shown in Image 15.



Image 14



Image 15

55. Around 4:45 p.m. EST, several minutes after DELUCA exited ST-2M, another rioter, Timothy Desjardins, circled in yellow in Image 16 below, picked up a wooden table leg in front of the Tunnel and used that leg to assault law enforcement officers. Simultaneously, another rioter picked up a table, circled in red, from the same location in front of the Tunnel. That rioter proceeded to throw the table at the officers in the Tunnel, as shown in Images 17 through 19 below. The table bears a strong resemblance to the table that DELUCA passed out of the window in Image 9 above, sharing the same design on the apron. But the table legs were broken off at some point in the melee.

56. Your affiant has reviewed correspondence and business records from the U.S. Senate Sergeant at Arms, which valued the replacement cost of the coffee table taken from ST-2M at approximately \$637.96.



Image 16



Image 17



Image 18



Image 19

57. Later that same day, at 5:53 p.m. EST, DELUCA messaged an acquaintance on Instagram, “It’s insanity here” and “I got maced and had a sound bomb go off right next to me.”

58. Over the next several days, DELUCA continued to post on social media about the riot at the U.S. Capitol. In the early morning hours of January 7, 2021, an Instagram user messaged DELUCA, “I’m wondering why you support the breaking into the capitol.” DELUCA responded, “According to the constitution it’s our house.”

59. On January 8, 2021, DELUCA commented on a post on Instagram: “I got maced pretty bad about three times, and on top of that it was extremely windy, so it was blowing everywhere. While I do believe some people were placed there to cause chaos I don’t believe that people were faking being maced. Even if they were not directly hit, the wind was carrying it and affecting everyone.” Several minutes later, DELUCA commented a second time saying, “I used milk to get the mace/tear gas out of my eyes. I’ve heard for some people holding onions near their eyes and nose can protect them from the tear gas. I’m not 100% sure tbh.”

60. On January 14, 2021, DELUCA issued a lengthy statement on social media about January 6. Among other things, DELUCA stated: “I was there on Jan. 6. I have mixed feelings. People went to the Capitol building because that’s Our House and that’s where we go to take our grievances. People feel, as do I that an election was stolen from them and it was allowed.”

61. On January 15, 2021, in an Instagram message, DELUCA suggested that the former president should declare martial law and overturn the election: “So it talks about how to save the election with all the fraud that’s happened. I can see from the notes that he suggests martial law. If Trump declares martial law in 7 states, his campaign allies could take control of the state’s ballots & overturn the results of the election in Trump’s favor. Which would be ideal.”

62. DELUCA also acknowledged deleting Instagram posts from her profile in the immediate aftermath of January 6. On January 9, 2021, an acquaintance messaged DELUCA on Instagram, “Not sure if this is right but your profile shows only 9 posts.” DELUCA replied, “Yes I deleted a lot of my posts.” Further review of DELUCA’s Instagram profile revealed there were no posts (as opposed to direct messages) between November 27, 2020 and January 11, 2021. Based on my knowledge, training, and experience, people who commit criminal acts will often delete information about those acts from social media accounts in an attempt to thwart any subsequent criminal investigation.

63. More recently, on December 5, 2023, your affiant interviewed employees of the apartment building located at [REDACTED], where DELUCA currently resides. Your affiant showed one of the employees a photograph of DELUCA from her Instagram account, and the employee positively identified the person in the photograph as DELUCA. You affiant then provided the same employee, who regularly sees DELUCA at the apartment building, with six photographs of DELUCA at the U.S. Capitol on January 6, 2021. The employee positively identified DELUCA in each of the six photographs. Additionally, through my own investigation, including reviewing DELUCA’s driver’s license photo, DELUCA appears to be the same person in the screenshots above and other video footage collected on January 6, 2021.

64. During this interview, the employees accessed the computer system for the apartment building located at [REDACTED], and queried DELUCA. The query confirmed that DELUCA currently resides at [REDACTED], with a roommate. The query also yielded a copy of DELUCA’s U.S. passport and leasing information confirming that DELUCA has inhabited the apartment since

on or about May 28, 2022. DELUCA's lease of the apartment is current through April 27, 2024. Moreover, DELUCA's bank records recently subpoenaed from JP Morgan Chase Bank in October 2023 reference a current address of [REDACTED]. Finally, the employee who identified DELUCA in photographs taken at the U.S. Capitol on January 6, 2021, regularly sees DELUCA at the PREMISES as part of her job duties.⁶

65. Based on the investigation, the amount of recording and photography that DELUCA appeared to do using a cell phone while inside the U.S. Capitol indicates a high likelihood that this information is still stored on the cellular device and/or other electronic devices owned by DELUCA. As described above, DELUCA appeared to take photos or record videos multiple times while at the U.S. Capitol on January 6, 2021. Accordingly, there is probable cause to believe that this evidence was on her cell phone and is likely to still be contained in her cell phone.

66. Further, based on the investigation, numerous persons committing the TARGET OFFENSES, including DELUCA, possessed digital devices to communicate with other individuals to plan their attendance in Washington D.C. on January 6, 2021, to coordinate with other participants at the gatherings there that day, and to communicate and post on social media

⁶ On February 28, 2024, the FBI learned from the building management that DELUCA has not used her key fob to gain entry into the building for the past two weeks. The FBI discovered that DELUCA is staying with an individual in Irvine, California and, at this time, has no known travel plans to return to Washington, D.C. But the FBI determined that DELUCA is still receiving mail at [REDACTED]. And according to the apartment building's records, DELUCA's lease is valid through April 27, 2024. The FBI has no reason to believe that she moved out of the premises.

and digital forums about the events of January 6 after they occurred. As described above, the FBI's investigation confirmed that DELUCA used social media, including Instagram and Twitter, to communicate with others about travel to Washington, D.C., and the events at the U.S. Capitol on January 6, 2021.

67. This is a likely scenario as virtually all adults in the United States use mobile digital devices. In a fact sheet from June 12, 2019, The Pew Research Center for Internet & Technology estimated that 96 percent of Americans owned at least one cellular phone, and that that same 2019 report estimated that 81 percent of Americans use at least one smartphone. *See* Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/> (last visited Jan. 9, 2021).

68. Based on my training and experience, I also know that some individuals who participated in the TARGET OFFENSES have been known to use anonymizing services and/or applications capable of encrypting communications to protect their identity and communications. By using such tools, in some cases, the only way to see the content of these conversations is on the electronic device that had been used to send or receive the communications.

69. Based on my training and experience, I know that when individuals acquire new cell phones, they commonly transfer data from their previous phone, including contact information, text messages, and photographs.

70. In addition, based on my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as the Apple iCloud service. Thus, there is reason to believe that evidence of the offense that

originally resided on DELUCA's cell phone may also be saved to other digital devices within the PREMISES.

71. Based on my training and experience, I also know that cell phones are expensive, and people routinely retain their cell phones for many months or years.

72. Based on a search of open-source records, the FBI discovered that DELUCA's cell phone number may have been XXX-XXX-5834 (the "5834 Number") around the time of January 6, 2021. During the investigation, the FBI lawfully obtained a search warrant from T-Mobile U.S., Inc. for the 5834 Number. The account for the 5834 Number was active on January 6, 2021, and registered to DELUCA's mother. Based on call records, DELUCA appeared to have used the 5834 Number as her cell phone with International Mobile Equipment Identity ("IMEI") [REDACTED]. In the early morning hours of January 6, 2021, the 5834 Number made calls originating from Baltimore, Maryland, which is consistent with DELUCA's travel itinerary and social media communications described above. During the day on January 6, 2021, the 5834 Number made and received several calls originating from Alexandria, Virginia, where DELUCA's hotel was located, and from several locations in Washington, D.C. near the U.S. Capitol. Instagram messages from DELUCA in January 2021 also confirm that she used the 5834 Number. According to records subpoenaed from T-Mobile, the account associated with the 5834 Number was subsequently terminated on February 8, 2021.

73. After February 2021, DELUCA's cell phone number appeared to be XXX-XXX-5223 (the "5223 Number"). According to the search warrant returns from Twitter, as of June 2022, DELUCA's Twitter account was associated with an Apple iPhone under the 5223 Number. Moreover, according to the search warrant returns from Instagram, DELUCA's Instagram account

was associated with an Apple iPhone under the 5223 Number. DELUCA also verified her Instagram account using the 5223 Number, meaning that the account holder responded to a text sent to the registered phone number. DELUCA's application to move into [REDACTED], also listed the 5223 Number under DELUCA's contact information. Records recently subpoenaed from T-Mobile U.S., Inc. confirm that the 5223 Number is registered to DELUCA's mother and is still active as of February 15, 2024. Until October 2023, the 5223 Number was an Apple iPhone 13 Pro Max with IMEI [REDACTED]. Beginning in or around October 2023 through February 15, 2024, the 5223 Number was an Apple iPhone 14 Plus with IMEI [REDACTED].

74. Based on evidence collected to date, numerous persons committing the TARGET OFFENSES at the U.S. Capitol on January 6, 2021, possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses. As described above, there is evidence that DELUCA possessed a mobile digital device while at the U.S. Capitol on January 6, 2021, using that device to record video and/or take photographs. There is also evidence that DELUCA used social media on that device to communicate with others about travel to Washington, D.C., and the events at the U.S. Capitol on January 6, 2021.

75. Based on my training and experience, individuals regularly keep their cell phones on their person or at their residence. Accordingly, there is probable cause to believe that DELUCA will be carrying one or more digital devices, including cell phones, on her person when the warrant is executed. There is also probable cause to believe that any devices not located on DELUCA's person at the time this warrant is executed would be located at the PREMISES.

76. The property to be searched includes laptop computers, digital devices, and/or tablets owned, used, or controlled by DELUCA, including but not limited to an Apple iPhone 14 Plus with IMEI [REDACTED], hereinafter the “Devices.” Your affiant has probable cause to believe that the Devices are currently located at [REDACTED], because DELUCA currently resides at this address.

77. Finally, your affiant understands that hundreds of people have been arrested in connection to the riot that occurred at the U.S. Capitol on January 6, 2021. During searches of many those people’s homes, from early 2021 through present, in multiple jurisdictions, law enforcement has recovered clothing, paraphernalia, tools, and digital devices that were worn, used, or carried on January 6, 2021.

78. For example, on July 28, 2023, a search of a defendant’s phone in the Southern District of Ohio yielded pictures and text messages pertaining to January 6, 2021. On October 9, 2023, a search warrant executed in the Western District of Wisconsin recovered clothing and gear worn by a defendant on January 6, 2021, including a ballistic vest and helmet, as well as a handwritten note about defecating in Nancy Pelosi’s office, and a phone, camera, and computer hard drive. In the Eastern District of Missouri, officers executed a search warrant on October 30, 2023, recovering cell phones and a laptop containing text messages and other written material that established the defendant’s conduct at the U.S. Capitol on January 6, 2021, which included assaulting police officers. On December 13, 2023, a search in the Northern District of West Virginia yielded two phones linked to January 6, 2021. In the Eastern District of California, a search warrant executed on December 15, 2023 recovered a cell phone with pictures taken by the defendant was at the U.S. Capitol on January 6, 2021. As recently as December 20, 2023, in the

Western District of Washington, law enforcement officers seized a defendant's cell phone containing text messages and images from January 6, 2021. Searches continue to provide evidence of the offense conduct on that day.

TECHNICAL TERMS

79. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global

positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data

security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A “modem” translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of

149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an

encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. “Malware,” short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

80. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus,

the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including DELUCA, use digital devices, like the mobile device used by DELUCA during her time at the U.S. Capitol on January 6, 2021, to, among other things, store images, videos, recordings, documents and records relating to their illegal activity, which can include logs of online chats; email correspondence; text or other “Short Message Service” (“SMS”) messages.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until

it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

81. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular,

records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information,

configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device during the commission of an offense, the individual's device will generally serve as a storage medium for evidence of the

crime. From my training and experience, I believe that a digital device used during the commission of a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

82. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,”

erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby

thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and

application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

83. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to determine whether

the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC ACCESS TO DEVICE(S)

84. This warrant permits law enforcement agents to obtain from the person of DELUCA (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person’s physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

85. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

86. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called

“Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

87. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.

88. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

89. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

90. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

91. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric

features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

92. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from DELUCA the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of DELUCA to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of DELUCA to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of DELUCA to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

93. The proposed warrant does not authorize law enforcement to require DELUCA to state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel DELUCA to state or otherwise provide that information. However, the voluntary disclosure of such information by DELUCA would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask DELUCA for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires DELUCA to

provide such information, and will make clear that providing any such information is voluntary and that DELUCA is free to refuse the request.

CONCLUSION

94. I submit that this affidavit supports probable cause for a warrant to search the PREMISES, as described in Attachment A-1, and DELUCA, as described in Attachment A-2, and to seize the items described in Attachment B.

Respectfully submitted,

[Redacted Signature]

Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on March 13, 2024.

2024.03.13

13:21:44 -04'00'

HON. ROBIN M. MERIWEATHER
UNITED STATES MAGISTRATE JUDGE