

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)
VARIOUS ELECTRONIC DEVICES BELONGING TO
ROGER J. STONE, JR.

Case: 1:19-sw-00057
Assigned To : Chief Judge Howell, Beryl A.
Assign. Date : 2/13/2019
Description: Search and Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the District of Columbia
(identify the person or describe the property to be searched and give its location):

See Attachment A.

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.

YOU ARE COMMANDED to execute this warrant on or before February 27, 2019 (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 Hon. Beryl A. Howell
(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

Date and time issued: February 13, 2019 at 4:40 PM Beryl A. Howell
Judge's signature

City and state: Washington, DC Hon. Beryl A. Howell, Chief U.S. District Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:	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 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*

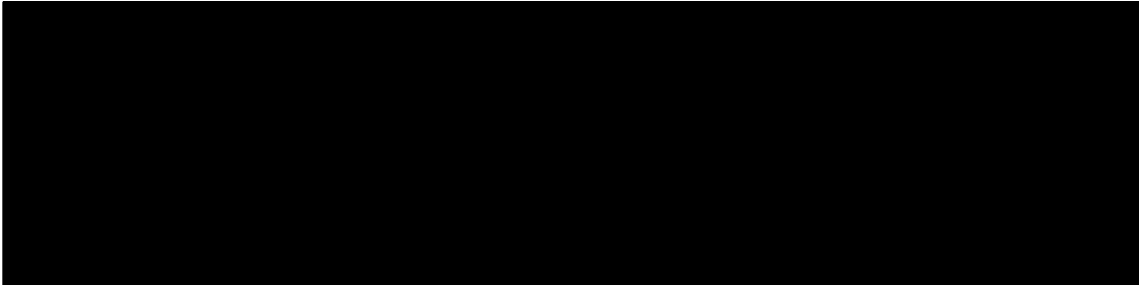
\_\_\_\_\_

*Printed name and title*

**ATTACHMENT A**

**Property to be Searched**

The following devices provided to the FBI by [REDACTED] currently in the District of Columbia:



**ATTACHMENT B**

**Items to be seized from the Subject Devices**

1. The items to be seized are fruits, evidence, information relating to, contraband, or instrumentalities of violations Title 18, United States Code, Section 1505 (obstruction of proceeding); (ii) Title 18, United States Code, Section 1001 (false statements); and (iii) Title 18, United States Code 1512(b)(1) (witness tampering), those violations involving Roger Stone, for the time period June 2015 to the present, including:

- a. Documents and communications that discuss or are related to WikiLeaks, Julian Assange, and/or Russian interference in the 2016 U.S. presidential election;
- b. Documents reflecting communications between Stone and Jerome Corsi;
- c. Documents reflecting communications between Stone and Randy Credico;
- d. Documents reflecting communications between Stone and members of the Trump Campaign or Trump Campaign associates, including Steve Bannon, [REDACTED] Paul Manafort, Richard Gates, and Donald J. Trump;
- e. Documents related to or discussing the U.S. House of Representatives Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, or the Federal Bureau of Investigation;
- f. Records and information relating to the e-mail account [REDACTED] n  
a [REDACTED];
- g. Records and information relating to the WhatsApp account associated with telephone number [REDACTED];
- h. Records and information relating to the Signal account associated with telephone number [REDACTED];

- i. Records and information relating to the Wickr account associated with telephone number [REDACTED];
  - j. Any computers, media storage devices, tablets/iPads, cellular telephones, smartphones, personal data assistant devices, or other electronic devices used to commit the violations described above or to store records or documents described above;
  - k. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes, notebooks, diaries, and reference materials, in whatever form;
  - l. Records pertaining to accounts held with Internet Service Providers or of Internet use, in whatever form;
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER 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 that would allow others to control the COMPUTER, 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 lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER'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;
- m. contextual information necessary to understand the evidence described in this attachment.

UNITED STATES DISTRICT COURT

for the  
District of Columbia

FILED  
FEB 13 2019

Clerk, U.S. District & Bankruptcy  
Courts 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)*  
VARIOUS ELECTRONIC DEVICES BELONGING TO  
ROGER J. STONE, JR.

)  
)  
)  
)

Case: 1:19-sw-00057  
Assigned To : Chief Judge Howell, Beryl A.  
Assign. Date : 2/13/2019  
Description: Search and Seizure Warrant

APPLICATION FOR A SEARCH WARRANT

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

located in the \_\_\_\_\_ District of \_\_\_\_\_ Columbia \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

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. § 1505	Obstruction of Proceeding
18 U.S.C. § 1512	Witness Tampering
18 U.S.C. § 1001	False Statements

The application is based on these facts:

See attached Affidavit.

- 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.

Reviewed by AUSA/SAUSA:

Aaron Zelinsky (ASC)

*Applicant's signature*

Curtis Heide, Special Agent, FBI

*Printed name and title*

Sworn to before me and signed in my presence.

Date: 02/13/2019

*Judge's signature*

City and state: Washington, D.C.

Hon. Beryl A. Howell, Chief U.S. District Judge

*Printed name and title*

**FILED**

FEB 13 2019

Clerk, U.S. District & Bankruptcy  
Courts for the District of Columbia

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF  
VARIOUS ELECTRONIC DEVICES  
BELONGING TO ROGER J. STONE, JR.

Case: 1:19-sw-00057  
Assigned To : Chief Judge Howell, Beryl A.  
Assign. Date : 2/13/2019  
Description: Search and Seizure Warrant

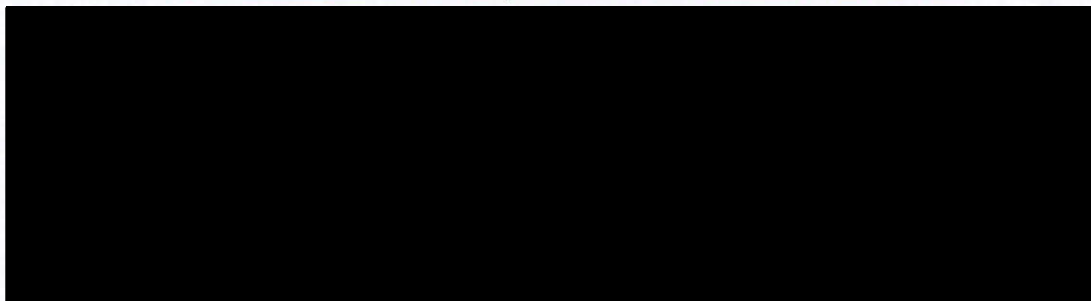
**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Curtis A. Heide, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for the following devices (the "Subject Devices") associated with Roger J. Stone, Jr. ("Roger Stone"), described below and further in Attachment A, currently located in the District of Columbia:

- a.
- b.
- c.



2. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been since 2006. In the course of my duties, I have been responsible for investigating federal crimes and national security matters involving both counterintelligence and issues related to cybersecurity.

3. I am currently involved in the investigation into Roger J. Stone, Jr., ("Roger Stone") and others known and unknown to the government, for the commission of unlawful activities in the District of Columbia, and elsewhere, including, but not limited to: (i) obstruction of proceeding, in violation of Title 18, United States Code, Section 1505; (ii) false statements, in



violation of Title 18, United States Code, Section 1001 and (iii) witness tampering, in violation of Title 18, United States Code 1512(b)(1) (collectively the “Specified Federal Offenses”).

4. On January 24, 2019, a Grand Jury in the District of Columbia indicted Roger Stone on seven counts: (i) obstruction of proceeding, in violation of Title 18, United States Code, Section 1505 (Count 1); (ii) false statements, in violation of Title 18, United States Code, Section 1001 (Counts 2-6) and; (iii) witness tampering, in violation of Title 18, United States Code 1512(b)(1) (Count 7). *See United States v. Roger Jason Stone, Jr.*, 19-cr-18-ABJ, Dkt. 1. On January 29, 2019, Roger Stone pled not guilty to the charges before Magistrate Judge Deborah A. Robinson.

5. I have personally participated in this investigation and am aware of the facts contained herein based on my own investigation, as well as my review of documents, records, and information provided to me by other law enforcement officers and technical experts.

6. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Unless specifically indicated, all conversations and statements in this affidavit are related in substance and part. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date specified.

7. For the reasons set forth in this Affidavit, there is probable cause to believe that one or more of the Specified Federal Offenses have been committed by Roger Stone and others known and unknown to the government. Further, there is probable cause to believe that each of the Subject Devices have been used to facilitate the commission of one or more of the Specified Federal Offenses. Moreover, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of the Specified Federal Offense may be present in each of the Subject Devices, as described further in Attachment B.

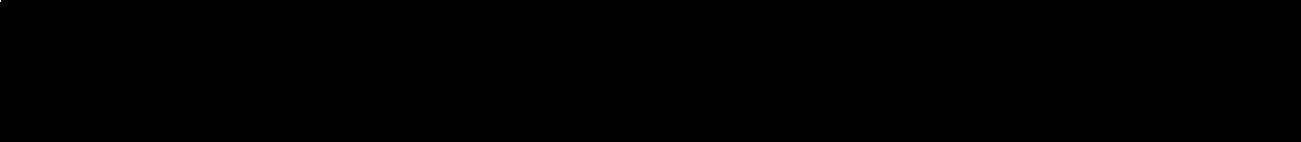
PROBABLE CAUSE

**A. Background on Relevant Individuals**

8. Roger Stone is a political consultant who has worked for decades in U.S. politics and on U.S. political campaigns. Stone was an official on the U.S. presidential campaign of Donald J. Trump (“Trump Campaign”) until in or around August 2015, and subsequently maintained regular contact with and publicly supported the Trump Campaign through the 2016 election.

9. Julian Assange is the founder and director of WikiLeaks, which is publicly described as a non-profit organization that disseminates non-public information and classified media provided by anonymized sources. WikiLeaks has posted numerous documents stolen from the U.S. government. At all relevant times, Assange was located at the Ecuadorian Embassy in London, United Kingdom.

10. Jerome Corsi is a political commentator who worked with an online media publication during the 2016 U.S. presidential campaign. As set forth below, Corsi spoke regularly with Stone throughout the campaign, including about the release of stolen documents by WikiLeaks.

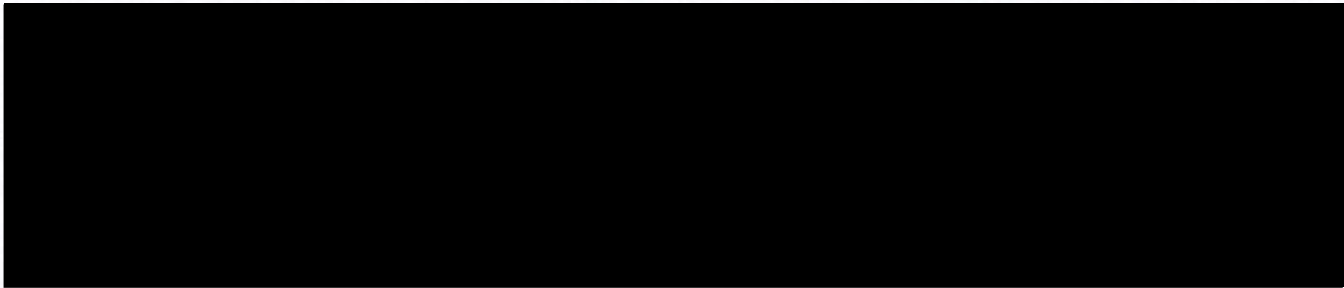


12. Based on the investigation to date, Randy Credico was a radio host who has known Stone for more than a decade. In testimony before the U.S. House of Representatives Permanent Selection Committee on Intelligence (“HPSCI”) on or about September 26, 2017, Stone described Credico (without naming him) as an “intermediary,” “go-between,” and “mutual friend” to Assange. In a follow-up letter to HPSCI dated October 13, 2017, Stone identified Credico by

name and claimed Credico was the “gentleman who confirmed for Mr. Stone” that Assange, had “[e]mails related to Hillary Clinton which are pending publication.”

13. Richard Gates is a U.S. citizen who served for years as a political consultant and lobbyist along with Paul Manafort. From in or around June 2016 until November 2016, Gates served as the deputy campaign chairman of the Trump Campaign. On February 23, 2018, Gates pled guilty to one count of conspiracy against the United States and one count of making false statements to federal law enforcement officers. *United States v. Gates*, 1:17-cr-201 (D.D.C.).

14. Steve Bannon is a U.S. citizen who serves as a political consultant. Beginning in or around August 2016 and through the 2016 U.S. presidential election, Bannon served as the chief executive officer of the Trump Campaign.



#### **B. Hacking Activity During the 2016 Presidential Election**

16. John Podesta is a U.S. citizen who served for years as a political consultant. During the 2016 U.S. presidential campaign, Podesta served as the campaign chairman of the Hillary Clinton presidential campaign (“Clinton Campaign”). On or about March 24, 2016, Podesta received a spearphishing<sup>1</sup> email designed to appear as a security notification (a partial copy of the email was recovered by the FBI from a subsequent release of stolen emails, described below). During an interview with the FBI in or around May 2018, Podesta indicated that after receiving

---

<sup>1</sup> In my training and experience, spearphishing in this context refers to the fraudulent practice of sending an email that purports to be from a known or trusted sender in order to induce the targeted victim to respond in a desired manner, typically by clicking a malicious link or URL.

the email, his assistant (who also had access to the account) clicked on a link within the email and entered the account password when prompted (believing this prompt to be part of a security protocol). Based on my training and experience, this activity appears to have been a successful spearphishing operation, through which an actor would have gained access to Podesta's email account, allowing the actor to steal emails and documents from that account.

17. The Democratic National Committee ("DNC") and Democratic Congressional Campaign Committee ("DCCC") are U.S. political committees focusing on U.S. federal elections. Both the DNC and DCCC were involved in the 2016 U.S. federal elections, including the 2016 U.S. presidential election. According to DNC and DCCC individuals interviewed by the Special Counsel's Office, in or around the spring of 2016, the DNC and DCCC became aware that their computer systems had been compromised by unauthorized intrusions and hired the cybersecurity company CrowdStrike to investigate the intrusions and remediate.

18. On or about June 14, 2016, CrowdStrike issued a public press release announcing that the DNC's computer network had been compromised. In the public statement, CrowdStrike indicated that it had identified "two sophisticated adversaries on the network," which it referred to by the monikers COZY BEAR and FANCY BEAR. CrowdStrike stated that it had previously seen these actors target other customers and that, based on their experience, "[b]oth adversaries engage in extensive political and economic espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services."

19. On or about July 13, 2018, a federal grand jury sitting in the District of Columbia returned an indictment against eleven Russian nationals, charging them with partaking in a conspiracy to hack into, among other things, the email account of John Podesta, as well as the

DNC and DCCC computer networks. *United States v. Viktor Borisovich Netyksho*, 1:18-cr-215 (D.D.C.). The indictment alleges that all of these individuals were military officers serving in the Main Intelligence Directorate of the General Staff (“GRU”), the Russian Federation’s military intelligence agency.

**C. WikiLeaks’ Release of Stolen Documents During the 2016 Presidential Campaign**

20. As alleged in the *Netyksho* indictment, after successfully hacking the DNC and DCCC networks, as well as Podesta’s email account, GRU officers transmitted some of the stolen documents to WikiLeaks. GRU officers communicated with WikiLeaks members about the transfers using online personas created by the GRU, including “Guccifer 2.0” and “DCLeaks.” (GRU officers separately used these personas to release some of the stolen documents).

21. On or about July 22, 2016, WikiLeaks released tens of thousands of documents stolen from the DNC network. These stolen documents included communications by senior DNC officials about campaign strategy, financial and fundraising data, and other documents related to the 2016 U.S. federal elections, including the 2016 U.S. presidential election.

22. Beginning in or around October 2016, WikiLeaks began to release tens of thousands of emails and documents stolen from Podesta’s email account. Between on or about October 7, 2016 and November 7, 2016, WikiLeaks released approximately 33 tranches of documents that had been stolen from John Podesta, releasing a total of over 50,000 documents.

**D. Stone’s Communications About WikiLeaks During the Campaign**

23. In April 2018 interviews with the Special Counsel’s Office, Richard Gates stated that starting in or around May 2016, when Gates was a senior official on the Trump campaign, Stone informed members of the Trump Campaign that WikiLeaks had emails from then-candidate Hillary Clinton. According to Gates, after the July 22, 2016 release of stolen DNC emails by

WikiLeaks, Gates observed a conversation between Manafort and Stone in which they discussed WikiLeaks and Stone's prediction of the release.

24. According to Gates, Manafort directed Gates to contact Stone about any additional releases and what other information WikiLeaks had regarding the Clinton Campaign. Gates contacted Stone, who made statements claiming that there would be potential future releases of damaging material by WikiLeaks. In a separate interview with the Special Counsel's Office in or around October 2018, Gates recalled that at one point during the campaign he was with then-candidate Trump in a car when the candidate had a telephone call with Stone; shortly after finishing the call with Stone, Gates recalled then-candidate Trump said more leaks were coming.

25. Emails recovered through a court-authorized search of Stone's email account [REDACTED] show that shortly after the July 22, 2016 release of stolen DNC emails by WikiLeaks, Stone corresponded with other associates about contacting WikiLeaks in order to obtain other emails damaging to the Clinton Campaign:

- a. On or about July 25, 2016, Stone sent an email to Jerome Corsi with the subject line, "Get to Assange." The body of the message read, "Get to Assange [a]t Ecuadorian Embassy in London and get the pending WikiLeaks emails . . . they deal with Foundation, allegedly." On or about the same day, Corsi forwarded

---

<sup>2</sup> A search of [REDACTED] was authorized on or about September 11, 2017 by the U.S. District Court for the District of Columbia. Case No. 1:17-mj-661 (D.D.C. Sept. 11, 2017). A second search of [REDACTED] was authorized on or about August 3, 2018 by the U.S. District Court for the District of Columbia. Case No. 1:18-sc-2582 (D.D.C. Aug. 3, 2018). On or about September 26, 2018, the government obtained and executed an order pursuant to 18 U.S.C. § 2703(d) for records connected to [REDACTED] Case No. 1:18-sc-2911 (D.D.C. Sept. 26, 2018). Records provided in response by Microsoft Corporation confirmed that the account was still active and that the relevant emails described in this affidavit were not deleted from the account.

Stone's email to [REDACTED] who lived in the United Kingdom and who was a supporter of the Trump Campaign.

- b. On or about July 31, 2016, Stone emailed Corsi with the subject line, "Call me MON." The body of the email read in part that [REDACTED] "should see Assange."
- c. On or about August 2, 2016, Corsi responded to Stone by email and wrote that he was currently in Europe and planned to return in mid-August. Corsi stated, "Word is friend in embassy plans 2 more dumps. One shortly after I'm back. 2nd in Oct. Impact planned to be very damaging." In a law enforcement interview, Corsi stated that the phrase "friend in embassy" referred to Assange. Corsi added in the same email, "Time to let more than Podesta to be exposed as in bed w enemy if they are not ready to drop HRC. That appears to be the game hackers are now about. Would not hurt to start suggesting HRC old, memory bad, has stroke – neither he nor she well. I expect that much of next dump focus, setting stage for Foundation debacle."

26. According to recorded public statements recovered by the FBI, starting in early August 2016, after receiving this August 2, 2016 email from Corsi, Stone made repeated statements about information he claimed to have learned from Assange:

- a. According to a public video posted to YouTube, on or about August 8, 2016, Stone attended a public event in Broward County, Florida. During the event, Stone stated, "I actually have communicated with Assange. I believe the next tranche of his documents pertain to the Clinton Foundation, but there's no telling what the October surprise may be."
- b. According to a public video posted to YouTube, on or about August 12, 2016, Stone was interviewed for a video segment on the show InfoWars, hosted by Alex Jones.

During the interview, Stone stated that he was “in communication with Assange” but was “not at liberty to discuss what I have.”

- c. According to a public video posted to YouTube, on or about August 16, 2016, Stone stated during another interview with Alex Jones that “it became known on this program that I have had some back-channel communications with WikiLeaks and Assange.” In a second interview on or about the same day with Dana Loesch of the TheBlaze TV, Stone stated that he “communicated with Mr. Assange” and that they had a “mutual acquaintance who is a fine gentleman.”
- d. According to a video posted to the public website of the TV station C-SPAN, during a C-SPAN television interview on or about August 18, 2016, Stone stated that he had communicated with Assange through an “intermediary, somebody who is a mutual friend.”
- e. In or around late 2018, Credico voluntarily produced to the FBI a copy of a radio interview he did with Stone on or about August 23, 2016 during which the two discussed Stone’s prior claims to be in contact with Assange. At one point during the interview, Credico asked Stone, “You’ve been in touch indirectly with Assange. Can you give us any kind of insight? Is there an October surprise happening?” Stone responded, “Well, first of all, I don’t want to intimate in any way that I control or have influence with Assange because I do not. . . . We have a mutual friend, somebody we both trust and therefore I am a recipient of pretty good information.”

27. In or around November 2018, [REDACTED], Stone produced a series of text messages between Stone and Credico during the 2016 presidential



campaign.<sup>3</sup> These text messages show that, beginning on or about August 19, 2016, Stone exchanged written communications with Credico about what WikiLeaks and Assange planned to do. Emails recovered through a court-authorized search of Stone's email account [REDACTED] show additional written communications between Stone and Credico about WikiLeaks in or around September 2016.

- a. On or about August 19, 2016, Credico sent a text message to Stone that read in part, "I'm going to have Julian Assange on my show next Thursday." On or about August 21, 2016, Credico sent another text message to Stone, writing in part, "I have Julian Assange on Thursday so I'm completely tied up on that day."
- b. On or about August 25, 2016, Assange was a guest on Credico's radio show for the first time. On or about August 26, 2016, Credico sent a text message to Stone that stated, "Assange talk[ed] about you last night." Stone replied and asked what Assange said, to which Credico responded, "He didn't say anything bad we were talking about how the Press is trying to make it look like you and he are in cahoots."
- c. On or about August 27, 2016, Credico sent text messages to Stone that said, "We are working on a Julian Assange radio show," and that he (Credico) was "in charge" of the project. In a text message sent later that day, Credico added, "Julian Assange has kryptonite on Hillary."
- d. On or about September 18, 2016, Stone sent a text message to Credico that said, "I am e-mailing u a request to pass on to assange." Credico responded "Ok," and

---

<sup>3</sup> As discussed below, Stone had previously released some of these text messages to members of the media, who had written about them and published them in part.

added in a later text message, “Just remember do not name me as your connection to Assange you had one before that you referred to.”

- e. Later on or about September 18, 2016, Stone emailed Credico an article with allegations against then-candidate Clinton related to her service as Secretary of State. Stone stated, “Please ask Assange for any State or HRC e-mail from August 10 to August 30 -- particularly on August 20, 2011 that mention [the subject of the article] or confirm this narrative.”
- f. On or about September 19, 2016, Stone texted Credico again, writing, “Pass my message . . . to Assange.” Credico responded, “I did.” On or about September 20, 2016, Credico forwarded the request to a close friend who was an attorney with the ability to contact the Assange. Credico blind-copied Stone on the forwarded email.
- g. On or about September 30, 2016, Credico sent Stone via text message a photograph of Credico standing outside the Ecuadorian Embassy in London where Assange was located.
- h. On or about October 1, 2016, which was a Saturday, Credico sent Stone text messages that stated, “big news Wednesday . . . now pretend u don’t know me . . . Hillary’s campaign will die this week.” In the days preceding these messages, the press had reported that Assange planned to make a public announcement on or about Tuesday, October 4, 2016, which was reported to be the 10-year anniversary of the founding of WikiLeaks.

- i. On or about October 2, 2016, Stone emailed Credico, with the subject line “WTF?” and a link to an article at the website <http://heatst.com/politics/october-surprise-thwarted-wikileaks-cancels-highly-anticipated-tuesday-announcement-due-to-security-concerns>. Credico responded to Stone, “head fake.”
- j. On or about Monday, October 3, 2016, Stone wrote Credico and asked, “Did Assange back off.” Credico initially responded, “I can’t tal[k] about it.” After further exchanges with Stone, Credico responded, “I think it[?]s on for tomorrow.” Credico added, “Off the Record Hillary and her people are doing a full-court press they [*sic*] keep Assange from making the next dump . . . That’s all I can tell you on this line . . . Please leave my name out of it.”

28. Emails and text messages recovered by the FBI show that, in or around October 2016, Stone made statements about Assange’s future releases that were similar to prior statements made by Credico to him. For example:

- a. In a court-authorized search of Stone’s email account [REDACTED] the FBI recovered an email from Stone to [REDACTED] sent on or about October 3, 2016, which stated in part, “Spoke to my friend in London last night. The payload is still coming.”
- b. In a court-authorized search of [REDACTED] the FBI also recovered an email exchange from on or about October 3, 2016 between Stone and a reporter who had connections to Bannon. In the exchange, the reporter asked, “Assange –

---

<sup>4</sup> A search of [REDACTED] was authorized on or about October 17, 2017 by the U.S. District Court for the District of Columbia. Case No. 1:17-mj-760 (D.D.C. Oct. 17, 2017). A second search of [REDACTED] was authorized on or about August 3, 2018 by the U.S. District Court for the District of Columbia. Case No. 1:18-sc-2583 (D.D.C. Aug. 3, 2018).

what's he got? Hope it's good." Stone responded, "It is. I'd tell Bannon but he doesn't call me back."

- c. On or about October 4, 2016, Assange held a press conference but did not release any new materials pertaining to the Clinton Campaign. In a court-authorized search of [REDACTED], the FBI recovered an email exchange between Stone and Steve Bannon on or about October 4, 2016 that occurred after the press conference. In the exchange, Bannon asked, "What was that this morning???", referring to Assange's press conference. Stone responded, "Fear. Serious security concern. He thinks they are going to kill him and the London police are standing do[wn]. However – a load every week going forward."
- d. In a court-authorized search of Stone's iCloud account,<sup>5</sup> the FBI recovered text messages between Stone and [REDACTED] from on or about October 4, 2016. In one text message [REDACTED] asked Stone if he had "hear[d] anymore from London." Stone replied, "Yes – want to talk on a secure line – got Whatsapp." In an interview with the Special Counsel's Office in or around May 2018 [REDACTED] confirmed that he and Stone spoke and that Stone had told him WikiLeaks had more material to release, and that the material was related to senior people associated with Clinton.

29. On or about October 7, 2016, WikiLeaks released the first set of emails stolen from Podesta. According to text messages recovered from Stone's iCloud account, shortly after the release, an associate of Bannon sent a text message to Stone that read "well done." Similarly,

---

<sup>5</sup> A search of Stone's iCloud account was authorized on or about March 14, 2018 by the U.S. District Court for the District of Columbia. Case No. 1:18-sc-662 (D.D.C. Mar. 14, 2018). The records for Stone's iCloud account contained some, but not all, of Stone's communications from the campaign period.

during an April 2018 interview, Gates recalled that after the October 7, 2016 WikiLeaks release, Stone said, “I told you this was coming.”

**E. Stone’s Communications with the House Permanent Select Committee on Intelligence**

30. On or about January 25, 2017, HPSCI publicly disclosed that it was investigating allegations of Russian interference in the 2016 presidential election and possible links to individuals associated with political campaigns.<sup>6</sup> During a public HPSCI hearing on or about March 20, 2017, multiple HPSCI committee members indicated that Stone’s prior public statements about having communications with Assange (particularly those from August 2016) were of interest to the committee.

31. In or around May 2017, HPSCI sent a letter requesting that Stone voluntarily appear before the committee and produce relevant documents to HPSCI (a copy of the HPSCI letter was recovered by the FBI from a court-authorized search of Stone’s email account players02@gmail.com). The letter requested Stone produce:

Any documents, records, electronically stored information including e-mail, communication, recordings, data and tangible things (including, but not limited to, graphs, charts, photographs, images and other documents) regardless of form, other than those widely available (e.g., newspaper articles) that reasonably could lead to the discovery of any facts within the investigation’s publicly-announced parameters.

32. On or about May 22, 2017, counsel for Stone responded to HPSCI in writing and stated that “Mr. Stone has no documents, records, or electronically stored information, regardless of form, other than those widely available that reasonably could lead to the discovery of any facts

---

<sup>6</sup> On or about January 13, 2017, the chairman and vice chairman of the Senate Select Committee on Intelligence (“SSCI”) announced the committee would conduct an inquiry that would investigate, among other things, any intelligence regarding links between Russia and individuals associated with political campaigns, as well as Russian cyber activity and other “active measures” directed against the United States in connection with the 2016 election.

within the investigation's publicly-announced parameters." (A copy of the letter was recovered from a court-authorized search of Stone's email account [REDACTED]).

#### **F. Stone's Testimony Before HPSCI**

33. On or about September 26, 2017, Stone provided HPSCI with an "opening statement" that his counsel requested be included as part of the record of proceedings before HPSCI. In his opening statement, which HPSCI provided to the Department of Justice,<sup>7</sup> Stone stated, "These hearings are largely based on a yet unproven allegation that the Russian state is responsible for the hacking of the DNC and John Podesta and the transfer of that information to WikiLeaks."

34. Also on or about September 26, 2017, Stone provided testimony in a closed session before HPSCI, at the U.S. Capitol in Washington, D.C. Stone's testimony was transcribed, and a copy of the transcript was obtained by the Special Counsel's Office from HPSCI in or around December 2018. Stone appeared before HPSCI under oath and affirmed for the record that he would tell the truth. At the beginning of the hearing, Stone was admonished that "it is unlawful to deliberately provide false information to Members of Congress or staff" and that "providing false information to this committee or concealing material information from this committee is a crime punishable by law."

#### **Stone's Testimony About Documents He Possessed Related to WikiLeaks**

35. During his HPSCI testimony, Stone was asked about HPSCI's May 2017 document

---

<sup>7</sup> On or about December 14, 2018, the U.S. Department of Justice requested the transcript of Stone's interview with HPSCI, as well as any written submissions and/or correspondence from Stone and/or his counsel before or after the interview. On or about December 20, 2018, HPSCI provided the U.S. Department of Justice a copy of the transcript of the September 26, 2017 interview of Roger Stone, a copy of Stone's written opening statement, and various correspondence from Stone's counsel to members of HPSCI.

request and whether Stone had any documents or written communications that discussed Julian Assange, Russian interference, or other relevant documents:

Q: The committee wrote to you on May 9th requesting no later than May 22 any documents, records, electronically stored information, including email communication, recordings, data, and other tangible things relevant to our investigation. You wrote back through counsel that you had no documents, records, or electronically stored information regardless of form responsive to our requests. Was that a false statement?

A: That is not a false statement. That's what -- I believe that to be true.

[. . .]

Q: So you have no emails to anyone concerning the allegations of hacked documents or your conversations with the Guccifer 2[.0] or any discussions you have had with third parties about Julian Assange? You have no emails, no texts, no documents whatsoever, any kind of that nature?

A: That is correct. Not to my knowledge. I think we met, again, the precise criteria of your request, and we complied. Again, if you have a more specific request, I'm happy to go back and look. . . .

Q: I just want to ask you under oath --

A: We did an extensive search consistent with the direction of my attorneys, and we found nothing that met the criteria that you asked for.

Q: I just want to be certain because you are under oath, where your letter was not under oath, that you have no documents, no emails, no texts, no tweets that refer to Julian Assange or Guccifer 2[.0] or Paul Manafort or the allegations concerning Russian connections with the campaign. You have had no discussions in any written form. You've written no documents yourself.

A: In connection with Russian collusion, consistent with your exact and precise request, yes.

36. In fact, and as described above, Stone had sent and received numerous emails and text messages during the 2016 campaign in which he discussed WikiLeaks, Assange, and

WikiLeaks possession of hacked emails. Court-authorized searches of Stone's email accounts (including [REDACTED]) and his iCloud account show that, at the time of his testimony, Stone was still in possession of many of these emails and text messages at the time he testified on or about September 22, 2017.<sup>8</sup> These written communications included (a) Stone's email to Corsi on or about July 25, 2016 that read in part, "Get to Assange [a]t Ecuadorian Embassy in London and get the pending WikiLeaks emails . . . they deal with Foundation, allegedly."; (b) Stone's email to Corsi on or about July 31, 2016 that [REDACTED] "should see Assange"; (c) Corsi's email to Stone on or about August 2, 2016 that stated in part, "Word is friend in embassy plans 2 more dumps. One shortly after I'm back. 2nd in Oct. Impact planned to be very damaging."; (d) dozens of text messages and emails between Stone and Credico, beginning on or about August 19, 2016 and continuing through duration of the election, in which they discussed WikiLeaks and Assange; (e) Stone's email to [REDACTED] on or about October 3, 2016 that read in part "Spoke to my friend in London last night. The payload is still coming."; and (f) Stone's email to Bannon on or about October 4, 2016 that claimed WikiLeaks would release "a load every week going forward."

*Stone's Testimony About His Early August 2016 Statements*

37. During his HPSCI testimony on or about September 26, 2017, Stone was asked to explain his statements in early August 2016 about being in contact with Assange. Stone was specifically asked about his statement on or about August 8, 2016 that "I've actually

---

<sup>8</sup> The warrant for Stone's email account [REDACTED] was obtained on or about September 11, 2017 and executed shortly thereafter. Records provided in or around September 2018 in response to a court order issued pursuant to 18 U.S.C. § 2703(d) confirmed that the account was active and the emails in question were not deleted from the account. The warrant for Stone's email account [REDACTED] was obtained on or about October 17, 2017 and executed shortly thereafter. The warrant for Stone's iCloud account (which contained the text messages described above) was obtained on or about March 14, 2018 and executed shortly thereafter.



communicated with Assange,” as well as his statement on or about August 12, 2016 that he was “in communication with Assange” but was “not at liberty to discuss what I have.”

38. Stone testified that these public references to having a means of contacting WikiLeaks referred exclusively to his contact with a journalist, who Stone described as a “go-between, as an intermediary, as a mutual friend” of Assange. Stone declined to tell HPSCI the name of this “intermediary,” but he provided a description in his testimony that was largely consistent with Credico. (On or about October 13, 2017, Stone caused a letter to be submitted to HPSCI that identified Credico by name as the “gentleman who confirmed for Mr. Stone” that Assange had “[e]mails related to Hillary Clinton which are pending publication.”).

39. In fact, documents recovered during the investigation (including those obtained via search warrant returns [REDACTED] show that Stone did not begin communicating with Credico about Assange or WikiLeaks until on or about August 19, 2016<sup>9</sup>—approximately eleven days after Stone first claimed on or about August 8, 2016 to “actually have communicated with Assange” and a week after his August 12, 2016 statements of being “in communication with Assange” and “not at liberty to discuss what I have.”

40. When interviewed by the FBI, Credico stated that the first time he ever spoke with Assange was on or about August 25, 2016, when Credico interviewed Assange.<sup>10</sup> Credico also provided the FBI with partially redacted emails that he claimed were between him and another

---

<sup>9</sup> As described above, on or about August 19, 2016, Credico informed Stone by text message that Credico intended to interview Assange the following week. On or about August 25, 2016, Credico interviewed Julian Assange for the first time, and on or about August 27, 2016, Credico texted Stone that “Assange has kryptonite on Hillary.”

<sup>10</sup> Credico was first interviewed by the FBI in or around August 2018. He has subsequently participated in multiple voluntary interviews [REDACTED]

member of WikiLeaks from on or about August 25, 2016, in which the two discuss the technical logistics for the interview later that day. During the exchange, Credico offered biographical information about himself, apparently as a means of introduction.

41. The FBI has not identified any communications between Stone and Credico from August 2016 in which Stone directs Credico to contact Assange or WikiLeaks. When interviewed by the FBI, Credico claimed he was never directed by Stone in August 2016 to contact WikiLeaks.

42. In contrast, and as described above, the FBI has identified written communications prior to August 8, 2016 in which Stone directed Corsi—not Credico—to contact Assange. On or about July 25, 2016, for example, Stone wrote to Corsi, “Get to Assange [a]t Ecuadorian Embassy in London and get the pending WikiLeaks emails . . . they deal with Foundation, allegedly.” Similarly, on or about August 2, 2016, Corsi—not Credico—sent an email to Stone in which Corsi wrote that “[w]ord is friend in embassy plans 2 more dumps,” including one in October. These communications occurred days before Stone’s first public statement on or about August 8, 2016 claiming to be in communication with Assange. However, at no time did Stone identify Corsi to HPSCI as another individual Stone contacted to serve as a “go-between,” “intermediary,” or other source for information from WikiLeaks. Similarly, Stone also never disclosed his written communications with Corsi to HPSCI when answering HPSCI’s questioning about the August 8, 2016 and August 12, 2016 statements about being in communication with Assange.

*Stone’s Testimony About Communications to Assange*

43. During his HPSCI testimony, Stone was asked, “Did you ask [the intermediary] to communicate anything else to Assange?” Stone responded, “I did not.” Stone was then asked, “Did you ask [the intermediary] to do anything on your own behalf?” Stone responded, “I did not.”

44. In fact, starting on or about September 18, 2016, Stone directed Credico to pass on a request to Assange for documents that Stone believed would be damaging to the Clinton Campaign.

- a. According to text messages obtained [REDACTED] on or about September 18, 2016, Stone sent a text message to Credico that said, “I am e-mailing u a request to pass on to Assange.” On or about the same day, Stone emailed Credico an article with allegations against then-candidate Clinton related to her service as Secretary of State. Stone added, “Please ask Assange for any State or HRC e-mail from August 10 to August 30 – particularly on August 20, 2011 that mention [the subject of the article] or confirm this narrative.” (A copy of this email was obtained through a search of Stone’s email account [REDACTED].)
- b. According to text messages obtained [REDACTED] on or about September 19, 2016, Stone texted Credico again, writing “Pass my message . . . to Assange.” Credico responded, “I did.” An email obtained from the account [REDACTED] shows that on or about September 20, 2016, Credico forwarded the request to an attorney who had the ability to contact Assange; Credico blind copied Stone on the same email.

Stone’s Testimony About Written Communications with Credico

45. During his HPSCI testimony, Stone was asked repeatedly about his communications with the person he identified as his intermediary. Stone stated that he had never communicated with his intermediary in writing in any way. During one exchange, Stone claimed only to have spoken with the intermediary telephonically:

Q: [H]ow did you communicate the intermediary?

A: Over the phone.

Q: And did you have any other means of communicating with the intermediary?

A: No.

Q: No text messages, no – none of the list, right?

A: No.

Later during his testimony, Stone again denied ever communicating with his intermediary in writing:

Q: So you never communicated with your intermediary in writing in any way?

A: No.

Q: Never emailed him or texted him?

A: He's not an email guy.

Q: So all your conversations with him were in person or over the phone.

A: Correct.

46. As described above, Stone and Credico (whom Stone identified as his intermediary) engaged in frequent written communication by email and text message. Beginning on or about August 19, 2016, and continuing through the 2016 U.S. presidential election, Stone and Credico engaged in dozens of communications by email or text message in which they discussed WikiLeaks and the possible release of stolen documents that would be damaging to the Clinton Campaign.

47. Written communications between Stone and Credico continued up until Stone's HPSCI testimony and afterwards. For example, on or about September 26, 2017—the day that Stone testified before HPSCI and denied having ever sent or received emails or text messages from his identified intermediary—Stone and Credico exchanged over thirty text messages.

48. Certain of the electronic messages between Stone and Credico (which Stone denied

ever taking place or possessing) would have been material to HPSCI, including Stone's messages in or around September 2016 directing Credico to pass a request for documents to Assange, and other relevant written communications with Credico. For example, on or about January 6, 2017, Credico sent Stone an email, which Stone had in his possession at the time of his HPSCI testimony, that had the subject line "Back channel bs." In the email, Credico wrote, "Well I have put together timelines[] and you [] said you have a back-channel way back a month before I had Assange on my show . . . I have never had a conversation with Julian Assange other than my radio show . . . I have pieced it all together . . . so you may as well tell the truth that you had no back-channel or there's the guy you were talking about early August." (A copy of this email was obtained through a search of Stone's email account [REDACTED]).

Stone's Testimony About Communications with the Trump Campaign

49. During his HPSCI testimony, Stone was asked, "[d]id you discuss your conversations with the intermediary with anyone involved in the Trump campaign?" Stone answered, "I did not." As described above, Stone spoke to multiple individuals involved in the Trump campaign about what he claimed to have learned from his intermediary to Assange, including the following:

- a. As described above, Gates confirmed to investigators that Stone spoke with senior Trump Campaign officials by telephone to inform them about materials possessed by Assange and the timing of future releases.
- b. According to text messages [REDACTED], on or about October 3, 2016, Stone wrote to [REDACTED], "Spoke to my friend in London last night. The payload is still coming."

- c. As described above, on or about October 4, 2016, after receiving information from Credico about the delay in WikiLeaks's release of stolen materials, Stone emailed Bannon that Assange had a "[s]erious security concern" but would release "a load every week going forward."

**G. Stone's Attempts to Influence Credico Regarding HPSCI and the FBI**

50. According to an email recovered through a court-authorized search of Stone's email account [REDACTED] on or about October 19, 2017, Stone sent Credico an excerpt of his October 13, 2017 letter to HPSCI in which Stone claimed Credico was his "intermediary" to Assange. As described below, Credico repeatedly told Stone that his letter was false and said he should correct his statement to HPSCI, but Stone did not do so. Stone then engaged in a prolonged effort to prevent Credico from contradicting Stone's false statements to HPSCI.

51. In or around November 2017, Credico received a request from HPSCI to testify voluntarily before the committee. After being contacted by HPSCI, Credico spoke and texted repeatedly with Stone. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- a. On or about November 19, 2017, Credico texted Stone that his lawyer wanted to see him. Stone responded, "Stonewall it. Plead the fifth. Anything to save the plan' . . . Richard Nixon." (A copy of these text messages was recovered through a court-authorized search of Stone's iCloud account). On or about November 20, 2017, Credico informed HPSCI that he declined HPSCI's request for a voluntary interview.

- b. On or about November 21, 2017, Credico texted Stone, “I was told that the house committee lawyer told my lawyer that I will be getting a subpoena.” Stone responded, “That was the point at which your lawyers should have told them you would assert your 5th Amendment rights if compelled to appear.” (A copy of these text messages was recovered through a court-authorized search of Stone’s iCloud account).
- c. On or about November 28, 2017, Credico received a subpoena compelling his testimony before HPSCI. Credico informed Stone of the subpoena.
- d. According to emails recovered from Stone’s email account [REDACTED] on or about November 30, 2017, Stone asked Corsi to write publicly about Credico. Corsi responded, “Are you sure you want to make something out of this now? Why not wait to see what [Credico] does? You may be defending yourself too much – raising new questions that will fuel new inquiries. This may be a time to say less, not more.” Stone responded by telling Corsi that Credico “will take the 5th—but let’s hold a day.”
- e. According to text messages recovered from Stone’s iCloud account, on multiple occasions, starting on or about November 17, 2017, Stone and Credico discussed Frank Pentangeli. Frank Pentangeli is a character in the film *The Godfather: Part II*, who falsely claims not to know critical information before a congressional committee that he does in fact know. On or about December 1, 2017, Stone told Credico in a text message to “Start practicing your Pentagele.” When interviewed by the FBI, Credico confirmed that he understood Stone’s references to Frank Pentangeli to be Stone’s way of suggesting Credico withhold relevant information

from investigators.

- f. On or about December 1, 2017, Stone texted Credico, “And if you turned over anything to the FBI you’re a fool.” Later that day, Credico texted Stone, “You need to amend your testimony before I testify on the 15th.” Stone responded, “If you testify you’re a fool. Because of trump I could never get away with a certain [*sic*] my Fifth Amendment rights but you can. I guarantee you you are the one who gets indicted for perjury if you’re stupid enough to testify.” (A copy of these text messages was recovered through a court-authorized search of Stone’s iCloud account).

52. On or about December 12, 2017, Credico informed HPSCI that he intended to assert his Fifth Amendment privilege against self-incrimination if required to appear by subpoena. According to Credico, he invoked his Fifth Amendment privilege in part to avoid providing evidence that would show Stone’s previous testimony to Congress was false.

53. Following Credico’s invocation of his Fifth Amendment privilege not to testify before HPSCI, Stone and Credico continued to have discussions about the various investigations into Russian interference in the 2016 election and what information Credico would provide to investigators. During these conversations, Stone repeatedly made aggressive statements intended to prevent Credico from cooperating with the investigations. For example:

- a. On or about December 24, 2017, Credico texted Stone, “I met assange for f[i]rst time this yea[r] sept 7 . . . docs prove that . . . You should be honest w fbi . . . there was no back channel . . . be honest.” Stone replied approximately two minutes later, “I’m not talking to the FBI and if your smart you won’t either.” (A copy of



these text messages was recovered through a court-authorized search of Stone's iCloud account).

- b. On or about April 9, 2018, Stone wrote in an email to Credico, "You are a rat. You are a stoolie. You backstab your friends—run your mouth my lawyers are dying Rip you to shreds." Stone also said he would "take that dog away from you," referring to Credico's dog. On or about the same day, Stone wrote to Credico, "I am so ready. Let's get it on. Prepare to die [expletive]." (A copy of this email exchange was recovered through a court-authorized search of Stone's email account [REDACTED]).
- c. On or about May 21, 2018, Credico wrote in an email to Stone, "You should have just been honest with the house Intel committee . . . you've opened yourself up to perjury charges like an idiot." Stone responded, "You are so full of [expletive]. You got nothing. Keep running your mouth and I'll file a bar complaint against your friend [the attorney who had the ability to contact the head of Assange]." (A copy of this email exchange was recovered through a court-authorized search of Stone's email account [REDACTED]). Credico believed Stone knew that Credico was sensitive to having this friend's name publicly disclosed.

#### **H. Missing Electronic Communications and Stone's Use of Encrypted Communications**

54. As described above, the government has recovered the content of many of Stone's electronic communications from summer and fall of 2016 (during the period of the U.S. presidential election) and afterward (during the period of pending congressional investigations into Russian interference in the U.S. election). However, the government is aware of the existence of

numerous other relevant electronic communications, the content of which it has not yet been able to recover.

55. As described above, during his HPSCI testimony, Stone falsely denied having emailed or exchanged text messages with his “intermediary” (later identified by Stone as Randy Credico). In fact, emails and text messages recovered in this investigation show the two communicated frequently by email and text messages; court-authorized searches of Stone’s email and iCloud accounts confirm that Stone still had those communications at the time he testified in or around September 2017. In numerous communications, Stone and Credico discussed Julian Assange and WikiLeaks, as well as Stone’s suggestion that Credico was his intermediary to Assange. These communications appear relevant and responsive to HPSCI’s inquiry, but Stone never disclosed them.

56. In addition to these emails and text messages in the FBI’s possession, the FBI has reviewed telephone billing records for Stone’s cellular telephone for the years 2016 and 2017, and they show text message communications whose content that the government to date has not been able to obtain. For example, these records indicate that Stone and Credico alone exchanged thousands of text messages (including over 1,500 text messages between the period November 2016 and December 2017) the substance of which the government to date has not recovered or reviewed. The government has only recently obtained text messages between Stone and Credico during some period of the campaign in 2016 from Stone’s subpoena production, issued after media reports in November 2018 stated that Stone’s attorneys were able to extract text messages between Stone and Credico from a phone Stone stopped using in 2016. But the government does not have, for the same time period, many of Stone’s other text messages. The government seeks these text messages believing they may show additional evidence of (1) the falsity of Stone’s HPSCI

testimony concerning his communications with his “intermediary” and (2) efforts to corruptly persuade Credico not to cooperate with pending investigations. As discussed further below, the government has reason to believe that these messages may be located on the Subject Devices.

57. Additionally, the FBI has interviewed multiple associates of Stone, who confirmed that Stone has used encrypted applications to communicate with others. Similarly, records obtained in this investigation indicate Stone uses multiple applications designed for encrypted communication, including (a) WhatsApp,<sup>11</sup> (b) Signal,<sup>12</sup> (c) Wickr,<sup>13</sup> and (d) ProtonMail.<sup>14</sup> To date, the FBI has not obtained any of Stone’s communications conducted through these applications.

---

<sup>11</sup> According to open sources, WhatsApp is an application that allows the user to send text messages, make voice calls, and transmit documents. WhatsApp uses end-to-end encryption and stores its messages separately from those text messages used on a mobile device’s default message application.

<sup>12</sup> According to open sources, Signal is an encrypted communications application allowing the user to send one-to-one and group messages, which can include files, voice notes, images and videos, and make one-to-one voice and video calls. Signal uses standard cellular mobile numbers as identifiers, and uses end-to-end encryption to secure all communications to other Signal users. Signal also allows users to set timers to messages, after which the messages will be deleted from both the sender’s and the receivers’ devices.

<sup>13</sup> According to open sources, Wickr is an instant messaging application that allows users to exchange end-to-end encrypted and content-expiring messages, including photos, videos, and file attachments and place end-to-end encrypted video conference calls. Like Signal, Wickr allows users to set an expiration time for their encrypted communications. In addition to encrypting user data and conversations, Wickr claims that its application strips metadata from all content transmitted through the network.

<sup>14</sup> According to open sources, ProtonMail is an end-to-end encrypted email service that uses client-side encryption to protect email contents and user data before they are sent to ProtonMail servers. According to its website, ProtonMail is run by Proton Technologies AG, a company based in the Canton of Geneva, and its servers are located at two locations in Switzerland, outside of US and EU jurisdiction.

- a. According to records from Stone's iCloud account, a copy of the WhatsApp application was downloaded to an iPhone registered to Stone on or about October 5, 2016. As described above, on or about October 4, 2016, Stone suggested in an email to [REDACTED] that they "talk on a secure line" and proposed using WhatsApp.
- b. According to records from Stone's iCloud account, a copy of the Signal application was downloaded to an iPhone registered to Stone on or about August 18, 2016. Additionally, text messages recovered from Stone's iCloud account revealed that on or about November 15, 2016, Stone sent an attorney with the ability to contact Julian Assange a link to download the Signal application.<sup>15</sup> Approximately fifteen minutes after sending the link, Stone texted the attorney, "I'm on signal just dial my number." The attorney responded, "I'll call you."
- c. According to records from Stone's iCloud account, a copy of the ProtonMail application was downloaded to an iPad registered to Stone on or about August 18, 2016.
- d. According to records from Stone's iCloud account, a copy of the Wickr application was downloaded to an iPhone registered to Stone on or about August 5, 2017.

58. Based on my training and experience, electronic communications using encrypted applications such as WhatsApp, Signal, ProtonMail, and Wickr are sometimes maintained on the device used to send and receive those communications. Communications from those applications can be obtained by law enforcement by searching the device either manually or via a data extraction device (such as Cellebrite). Searches of the physical device can reveal messages,

---

<sup>15</sup> This attorney was a close friend of Credico's and was the same friend Credico emailed on or about September 20, 2016 to pass along Stone's request to Assange for emails connected to the allegations against then-candidate Clinton related to her service as Secretary of State.

including text messages and messages exchanged over WhatsApp, Signal, ProtonMail, and Wickr, that have not been backed up to cloud accounts (such as an iCloud account). Additionally, review of the device and the downloaded application can reveal other evidence of encrypted communications, such as call logs and contact lists.

59. The FBI continues to seek evidence of Stone's communications and contacts during the period of the 2016 U.S. presidential election and through the present. The FBI believes these communications may contain evidence of additional communications concerning Assange, WikiLeaks, and the release of stolen documents damaging to the Clinton Campaign. Such communications could constitute additional evidence of Stone's efforts to obstruct HPSCI's investigation by showing additional contacts and communications about Assange and WikiLeaks that Stone failed to disclose.

#### **I. The Subject Devices**

60. In or around November 2018, media reports began to publish excerpts of text messages between Stone and Randy Credico that occurred during the 2016 U.S. election (copies of these text messages subsequently were obtained from Stone [REDACTED]).<sup>16</sup> According to these news articles, Stone released these messages to the media outlets, which Stone claimed were extracted by his lawyers from "a cell phone he stopped using in 2016." Based on these statements and described further below, your affiant believes the cell phone referenced in the article to be the iPhone 5s.<sup>17</sup>

---

<sup>16</sup> See, e.g., "Bombshell Text Messages Support Roger Stone's Claims About WikiLeaks Backchannel," Daily Caller, Nov. 14, 2018, available at <https://dailycaller.com/2018/11/14/roger-stone-wikileaks-randy-credico-mueller>.

[REDACTED] a, Stone produced some text messages between Credico and him; the latest-in-time text message produced by Stone occurred on or about November 14, 2016.

61. On or about February 11, 2019, investigators, with the consent of Roger Stone's attorneys, spoke with [REDACTED], a certified forensic examiner who stated he had been retained by Roger Stone's attorneys. [REDACTED] had been authorized by Stone's attorneys to provide the Subject Devices to the FBI, although in providing the devices, Stone did not consent to their search. Stillman gave the Agents three devices: the iPhone 5s, the iPhone 7, and the external hard drive.

62. [REDACTED] produced documentation to investigators indicating that the iPhone 5s was associated with the phone number ending in [REDACTED] Stone's cellular number as discussed above. The documentation also indicated that [REDACTED] had imaged the iPhone 5s on or about November 10, 2018, several days before the article discussed above where Stone claimed to have released newly-uncovered messages with Credico. Toll records produced by AT&T pursuant to subpoena indicate that Stone used an iPhone 5s from at least on or about January 1, 2015 through on or about November 14, 2016. Therefore, it appears that the iPhone 5s was the device Stone was using through November 14, 2016 to communicate with individuals including Credico and Corsi.

63. [REDACTED] also produced documentation to investigators that the iPhone 7 he provided to investigators was associated with the same Stone phone number ending in [REDACTED]. As discussed above, toll records produced by AT&T pursuant to subpoena indicate that Stone used an iPhone 7 from at least on or about November 14, 2016 through on or about February 25, 2018. As described above, Stone communicated extensively with Credico during this time. Toll records also indicate Stone continued to communicate with Corsi during this time period using the x3034 number.

---

The government believes copies of later-in-time text messages from late 2016 and early 2017 could be located on another device, such as the iPhone 7, or on backup storage media.

64. [REDACTED] further told investigators that the external hard drive contained forensic images of Stone's computers. [REDACTED] stated that the hard drive contained backups created by a separate company in September 2017 from Stone's computers in both Florida and New York. According to [REDACTED] the backups were created as "clone copies," which are copies of Stone's computer systems. [REDACTED] also indicated that the drive contained a separate image [REDACTED] created in March 2018 of Stone's computer in Florida, as well as backup images of the iPhones discussed above. As explained further herein, there is reason to believe that these images contain communications made by Stone with Credico, Corsi, and others made during the relevant time period, even if such communications had previously been deleted.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

65. As described herein and in Attachment B, this application seeks permission to search the Subject Devices. One form in which the records might be found is data stored on a device's hard drive. Thus, the warrants applied for would authorize the search of electronic storage media.

66. *Probable cause.* I submit that there is probable cause to believe those records will be stored on the Subject Devices (the term "computer" below refers to Subject Devices), for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a

computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

67. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Subject Devices because:



- a. Data on the storage medium 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 traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and

malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contains information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a thumb drive). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping"

program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers 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 storage medium 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, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer 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 a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.


FILTER REVIEW PROCEDURES

Review of the items described in Attachment B will be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges. The procedures include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

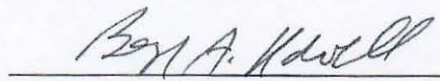
CONCLUSION

68. Based on the foregoing, your affiant respectfully requests that this Court issue a search warrant for the Subject Devices, more particularly described in Attachment A authorizing the seizure of the items described in Attachment B.

Respectfully submitted,

  
Curtis A. Heide  
Special Agent  
Federal Bureau of Investigation

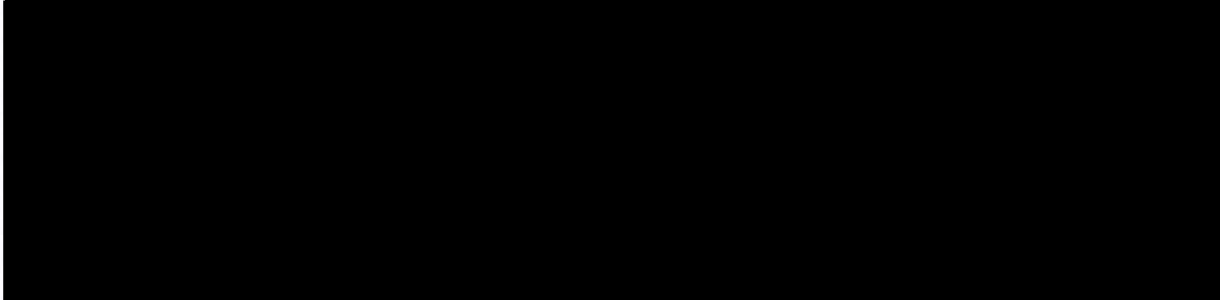
Sworn and subscribed before me on this 13<sup>th</sup> day of February, 2019.

  
The Honorable Beryl A. Howell  
Chief United States District Judge

ATTACHMENT A

Property to be Searched

The following devices provided to the FBI by [REDACTED], currently in the District of Columbia:



ATTACHMENT B

Items to be seized from the Subject Devices

1. The items to be seized are fruits, evidence, information relating to, contraband, or instrumentalities of violations Title 18, United States Code, Section 1505 (obstruction of proceeding); (ii) Title 18, United States Code, Section 1001 (false statements); and (iii) Title 18, United States Code 1512(b)(1) (witness tampering), those violations involving Roger Stone, for the time period June 2015 to the present, including:
  - a. Documents and communications that discuss or are related to WikiLeaks, Julian Assange, and/or Russian interference in the 2016 U.S. presidential election;
  - b. Documents reflecting communications between Stone and Jerome Corsi;
  - c. Documents reflecting communications between Stone and Randy Credico;
  - d. Documents reflecting communications between Stone and members of the Trump Campaign or Trump Campaign associates, including Steve Bannon, [REDACTED] Paul Manafort, Richard Gates, and Donald J. Trump;
  - e. Documents related to or discussing the U.S. House of Representatives Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, or the Federal Bureau of Investigation;
  - f. Records and information relating to the e-mail accounts [REDACTED] and p [REDACTED];
  - g. Records and information relating to the WhatsApp account associated with telephone number [REDACTED];

- h. Records and information relating to the Signal account associated with telephone number [REDACTED]
- i. Records and information relating to the Wickr account associated with telephone number [REDACTED]
- j. Any computers, media storage devices, tablets/iPads, cellular telephones, smartphones, personal data assistant devices, or other electronic devices used to commit the violations described above or to store records or documents described above;
- k. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes, notebooks, diaries, and reference materials, in whatever form;
- l. Records pertaining to accounts held with Internet Service Providers or of Internet use, in whatever form;
- 2. For all of the devices listed in Attachment A (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER 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 that would allow others to control the COMPUTER, 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 lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER'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;
- m. contextual information necessary to understand the evidence described in this attachment.