	Versions 1-9	Version 10	Version 11	Version 12	Versions 13-14
Language in Affidavit	In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:	(4) In searching for data capable of being read, stored or interpreted by a digital device, law enforcement personnel executing this search warrant will employ the following procedure:	In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing the search warrant for the SUBJECT PREMISES will employ the following procedure:	[*SAME AS VERSIONS 1-9*] In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:	[*SAME AS IN VERSION 10*] (4) In searching for data capable of being read, stored or interpreted by a digital device, law enforcement personnel executing this search warrant will employ the following procedure:
	(a) Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.	(i) Upon securing the premises, the law enforcement personnel executing the search warrant will, to the extent possible without requiring the use of special training in searching and seizing digital data, seek to determine if any digital device contains data falling within the scope of the items to be seized in the warrant. If they can make this determination without jeopardizing the integrity of the digital data and a digital device contains data falling within the scope of the items to be seized in the warrant, that digital device will be seized. If they cannot make this determination, or they believe they cannot make this determination, without jeopardizing the integrity of the digital data, law enforcement personnel trained in searching and seizing digital data (the "computer personnel") will be consulted (either on-site or off-site) to determine whether the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data contained on the digital device.	[*SAME AS IN VERSIONS 1-9*] (a) Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.	[*SAME AS VERSIONS 1-9, 11*] (a) Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.	[*SAME AS IN VERSION 10*] (i) Upon securing the premises, the law enforcement personnel executing the search warrant will, to the extent possible without requiring the use of special training in searching and seizing digital data, seek to determine if any digital device contains data falling within the scope of the items to be seized in the warrant. If they can make this determination without jeopardizing the integrity of the digital data and a digital device contains data falling within the scope of the items to be seized in the warrant, that digital device will be seized. If they cannot make this determination, or they believe they cannot make this determination, without jeopardizing the integrity of the digital data, law enforcement personnel trained in searching and seizing digital data (the "computer personnel") will be consulted (either on-site or off-site) to determine whether the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data contained on the digital device.
	No similar section	(ii) If the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, it will be searched on-site and seized only if the search reveals it to contain any data that falls within the list of items to be seized set forth herein.	No similar section	No similar section	[*SAME AS IN VERSION 10*] (ii) If the digital device can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, it will be searched on-site and seized only if the search reveals it to contain any data that falls within the list of items to be seized set forth herein.
	(b) If the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.	(iii) If the digital device cannot be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, then the computer personnel will determine whether it is practical to create a forensically sound image of the data contained on the digital device during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve that data. If it is practical, and the digital device cannot be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the computer personnel will make a forensically sound image of the data contained on the digital device (a "data image") during the execution of this search and shall seize the data image rather than the digital device itself.	[*SAME AS IN VERSIONS 1-9*] (b) If the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.	[*SAME AS IN VERSIONS 1-9, 11*] (b) If the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.	[*SAME AS IN VERSION 10*] (iii) If the digital device cannot be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, then the computer personnel will determine whether it is practical to create a forensically sound image of the data contained on the digital device during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve that data. If it is practical, and the digital device cannot be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the computer personnel will make a forensically sound image of the data contained on the digital device (a "data image") during the execution of this search and shall seize the data image rather than the digital device itself.
	(c) If the computer personnel determine it is not practical to perform an on-site search or make an on-site copy of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. [*THIS IS WHERE LANGUAGE IN VERSION 1 BEGAN*] The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized and set forth herein.	(iv) If the computer personnel determine it is not practical to perform an on-site search of the digital device or make an on-site data image within a reasonable period of time and without jeopardizing the ability to preserve the data, then the digital device will be seized and transported to an appropriate law enforcement laboratory for review. The digital devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized and set forth herein.	[*SAME AS IN VERSIONS 1-9*] (c) If the computer personnel determine it is not practical to perform an on-site search or make an on-site copy of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized and set forth herein.	[*SAME AS VERSIONS 1-9, 11*] (c) If the computer personnel determine it is not practical to perform an on-site search or make an on-site copy of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized and set forth herein.	[*SAME AS IN VERSION 10*] (iv) If the computer personnel determine it is not practical to perform an on-site search of the digital device or make an on-site data image within a reasonable period of time and without jeopardizing the ability to preserve the data, then the digital device will be seized and transported to an appropriate law enforcement laboratory for review. The digital devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized and set forth herein.
	(d) In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.	(v) In searching the digital device or data image[], the computer personnel may examine all of the data contained in the digital device or data image to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.	[*SAME AS IN VERSIONS 1-9*] (d) In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.	[*SAME AS VERSIONS 1-9, 11*] (d) In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.	[*SAME AS IN VERSION 10*] (v) In searching the digital device or data image[], the computer personnel may examine all of the data contained in the digital device or data image to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.
	(e) If the computer personnel do not determine that the data falls within any of the items to be seized pursuant to this warrant, the government will return the original data storage devices within a reasonable period of time not to exceed 60 days from the date of execution of the warrant. If the government needs additional time to determine whether the data falls within any of the items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original sixty day period.	(vi) If the computer personnel seize the digital device pursuant to subparagraph iv above or make a data image pursuant to subparagraph iii above, the computer personnel will initially search the digital device or data image within a reasonable amount of time not to exceed 60 days from the date of execution of the warrant. If, after conducting such an initial search, the case agents determine that the digital device or data image contains any data falling within the list of items to be seized pursuant to this warrant, the government will either (1) return the digital device, keeping a data image for further analysis, provided that, prior to such return, the owner and user(s) of the digital device stipulate individually and in writing to the authenticity and accuracy of the data image or (2) seek an order of the Court allowing the government to retain the original digital device for further analysis. If the digital device or data image does not contain any data falling within the list of the items to be seized pursuant to this warrant, the government will return the digital device or delete the data image. If the government needs additional time to determine whether the digital device or data image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original sixty day period from the date of execution of the warrant.	[*SAME AS IN VERSIONS 1-9*] (e) If the computer personnel do not determine that the data falls within any of the items to be seized pursuant to this warrant, the government will return the original data storage devices within a reasonable period of time not to exceed 60 days from the date of execution of the warrant. If the government needs additional time to determine whether the data falls within any of the items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original sixty day period.	[*SAME AS VERSIONS 1-9, 11*] (e) If the computer personnel do not determine that the data falls within any of the items to be seized pursuant to this warrant, the government will return the original data storage devices within a reasonable period of time not to exceed 60 days from the date of execution of the warrant. If the government needs additional time to determine whether the data falls within any of the items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original sixty day period.	[*SAME AS IN VERSION 10*] (vi) If the computer personnel seize the digital device pursuant to subparagraph iv above or make a data image pursuant to subparagraph iii above, the computer personnel will initially search the digital device or data image within a reasonable amount of time not to exceed 60 days from the date of execution of the warrant. If, after conducting such an initial search, the case agents determine that the digital device or data image contains any data falling within the list of items to be seized pursuant to this warrant, the government will either (1) return the digital device, keeping a data image for further analysis, provided that, prior to such return, the owner and user(s) of the digital device stipulate individually and in writing to the authenticity and accuracy of the data image or (2) seek an order of the Court allowing the government to retain the original digital device for further analysis. If the digital device or data image does not contain any data falling within the list of the items to be seized pursuant to this warrant, the government will return the digital device or delete the data image. If the government needs additional time to determine whether the digital device or data image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original sixty day period from the date of execution of the warrant.
	(2nd SECTION #; see Notes below) In order to search for data that is capable of being read or interpreted by a digital device, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above: . . .	(5) In order to search for data that is capable of being read or interpreted by a digital device, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above: . . .	[*SAME AS IN VERSIONS 1-9*] In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above: . . .	[*SAME AS IN VERSIONS 1-9, 11*] In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above: . . .	[*SAME AS IN VERSION 10*] (5) In order to search for data that is capable of being read or interpreted by a digital device, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above: . . .
See pages	Version 1: (Starting on Missing Page 26)-AFFIDAVIT_000027 Version 2: AFFIDAVIT_000059-62 Version 3: AFFIDAVIT_000096-99 Version 4: AFFIDAVIT_000133-36 Version 5: AFFIDAVIT_000170-73 Version 6: AFFIDAVIT_000210-13 Version 7: AFFIDAVIT_000248-51 Version 8: AFFIDAVIT_000288-91 Version 9: AFFIDAVIT_000328-331	AFFIDAVIT_000413-418	AFFIDAVIT_000455-458	AFFIDAVIT_000512-515	Version 13: AFFIDAVIT_000555-560 Version 14: AFFIDAVIT_000599-604

PAGE 000707

EXHIBIT K

Case 2:10-cr-01031-AM Document 632-27 Filed 07/25/11 Page 1 of 1 Page ID #:17246