

UNITED STATES DISTRICT COURT

District of _____

In the Matter of the Search of

(Name, address or brief description of person or property to be searched)

SEARCH WARRANT

Hysen Sherifi, et al
1320 E Steinbeck Drive
Raleigh, North Carolina

Case Number: 05-09-MH1022

TO: Federal Bureau of Investigation and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent Michael A. Greer who has reason to believe
Affiant

that on the person of, or on the premises known as (name, description and/or

As described in Attachment A

in the Eastern District of North Carolina there is now
concealed a certain person or property, namely (describe the person or property)

Items described in Attachment B.
Any computer search shall be conducted in accordance with Attachment C.

I am satisfied that the affidavit(s) and any record testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before 4 August 2009
Date

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search in the daytime — 6:00 AM to 10:00 P.M. at anytime in the day or night as I find reasonable cause has been established and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to

ANY E.O.N.C. MAGISTRATE JUDGE as required by law.

U.S. Magistrate Judge (Rule 41 (f)(4))

25 JULY 2009 4:00 pm
Date and Time Issued

Raleigh, NC
City and State

James E. Gates, U.S. Magistrate Judge
Name and Title of Judge

[Signature]
Signature of Judge

RETURN		Case Number: 415M-CE-9391B (5:09-CR-216-7-FL)
DATE WARRANT RECEIVED 7/25/2009	DATE AND TIME WARRANT EXECUTED 7/27/2009, 11:54	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH left at residence

INVENTORY MADE IN THE PRESENCE OF
Nobody Present at residence.

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

SEE ATTACHED

FILED
JUL 30 2009
DENNIS P. IAVARONE, CLERK
US DISTRICT COURT, EDNC
BY AAA DEP CLK

CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

[Signature] **415M**

Subscribed, sworn to, and returned before me this date.

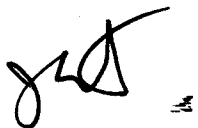
Michael A. Greer
Signature of Judge

7/30/09
Date

Attachment A

Description of location(s) to be searched:

1320 E Steinbeck Drive, Raleigh, NC 27609, is an apartment in the Tree Top Apartment complex on Steinbeck Drive. 1320 E is in a building inside the second entrance to the Tree Top Apartment complex and is located toward the end of the parking lot. 1320 E is an upstairs apartment and faces the front of the unit.

Handwritten signature or initials in the bottom right corner of the page.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED

Based on the facts as recited in the attached affidavit, your Affiant has probable cause to believe that the following items containing or constituting evidence, fruits and instrumentalities of violations of Title 18, United States Code 2339A, 956(a), and 924(c), are at the location described in Attachment A.

Items sought to be seized include, but are not limited to the following, but seizure is permitted only to the extent such items constitute or contain evidence, fruits and instrumentalities of violations of the described crimes:

1. Any and all records, documents and materials. The term "records," "documents," and "materials" include all of the following items of evidence in whatever form and by whatever means such records, documents or materials, their drafts, or their modifications may have been created or stored, including, but not limited to, any handmade form (such as writing or drawing with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact discs or any information on an electronic or magnetic storage device, such as floppy diskettes, hard drives, CD-ROMs, DVDs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives or electronic notebook, as well as printouts or readouts from any magnetic storage device).
 - a. Any and all past or present telephone books, Rolodex indices, calendars, telephone bills, appointment books, and other documents reflecting appointment and/or names, addresses and/or telephone numbers.
 - b. Any and all notes, markings, papers, paper scraps, partial documents, fax records, electronic mail, or other materials.
 - c. Identification documents, including but not limited to documents and other evidence that indicate ownership, occupancy, residency and associations.
 - d. Any and all financial and bank statements and records, money drafts, letters of credit, cashier's checks, safe deposit keys, statements of accounts, returned or cancelled checks, checkbooks and stubs, duplicates and copies of checks, deposit items, savings books, and passbooks, and similar bank and financial records.
2. Any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, modems, tape drives, disk application programs, data disks, system



disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals

3. Any and all firearms, ammunition, explosives, explosive components and accessories, including but not limited to, hand guns, long guns, ammunition, ammunition containers, optics, magazines, and firearm accessories.
4. Any and all photographs, books, videos, and literature that advocates violent jihad, depicts potential co-conspirators or criminal associations, and depicts potential targets.
5. Currency.
6. Cellular telephones and SIM cards (cellular phone memory chip).

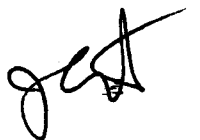
gest

**ATTACHMENT C TO SEARCH WARRANT
COMPUTER SEARCH PROTOCOL**

1. Definition of "Computer." Unless otherwise defined in the warrant, "computer" means any electronic, magnetic, optical, electro-chemical, or other data processing device performing logical or storage functions, and includes any information storage facility, communications facility, or other equipment or media directly related to or operating in conjunction with such device. "Computer" also includes the system software (*e.g.*, operating systems, interfaces, hardware drivers), applications software, and related instruction manuals or other documentation and data security devices (*e.g.*, passwords, keycards) needed to conduct the search authorized by the warrant. "Media" as used in this definition means all forms of material or devices that are capable of storing or preserving electronic information (*i.e.*, data of any kind).

2. On-Site Search. To the extent practicable, the computer described in the warrant shall be analyzed at the search site (*i.e.*, the location identified in the warrant) and not seized for analysis off-site. Alternatives to seizure for purposes of analysis off-site that may be considered by the government include, but are not limited to, the following:

- (a) identification of a knowledgeable person at the search site who could assist the government in locating information subject to the warrant;
- (b) use by the government of its own expert at the search site to locate the information subject to the warrant;
- (c) creation at the search site of an electronic mirror image of those parts of the computer that are likely to contain information subject to the warrant and subsequent analysis of such mirror image copy off-site in lieu of the computer.



3. Seizure for Analysis Off-Site. If any computer subject to the warrant cannot practicably be analyzed at the search site, the warrant allows for seizure of such computer and its removal from the search site to a laboratory, controlled environment, or other off-site location for purposes of analysis. Such off-site analysis shall be completed as promptly as practicable. In the event of such seizure, the government shall furnish to the issuing Magistrate Judge every 30 calendar days after the warrant is returned a status update regarding the analysis being conducted, including an estimate of the additional time needed to complete the analysis. These updates shall continue to be submitted until the analysis is complete or until further order of the court. If upon completion of the off-site analysis the government determines that the computer and the information stored in it are not subject to permanent seizure as contraband (*i.e.*, property used in furtherance of criminal activity), fruits of criminal activity, or on other grounds, the government shall return the computer to the person from whom or from whose premises it was taken. Such return shall be made as soon as practicable after completion of the analysis but in no event more than 10 calendar days thereafter unless a longer time is allowed by court order or agreement of the parties.

4. Seizure as Contraband or Instrumentality. The government may permanently seize a computer and information stored therein that the government identifies (in connection with either an on-site or off-site search) as contraband, fruits of criminal activity, or otherwise subject to permanent seizure if the warrant allows for such permanent seizure. If the warrant does not authorize such permanent seizure, the government shall obtain another warrant supported by probable cause authorizing permanent seizure before effecting it. If the computer had initially been seized only for purposes of analysis off-site, the government shall notify the issuing Magistrate Judge of its determination to permanently seize the computer and/or information stored therein and may request



that its ongoing obligation to report on its analysis of such computer cease.

5. Storage of Information on Seized Computer. The government shall make a copy of all information stored on the computer as soon as practicable after the computer's seizure except as otherwise provided by the warrant. Such copy shall not be analyzed by the government except as reasonably necessary to confirm that it is an accurate copy, but shall be retained until further order of the court as a record of the state of the computer and the information therein prior to any subsequent analysis by the government. **The government shall not reconfigure the computer until such copy has been made.**

6. Return of Information from Seized Computer. If any person from which or from whose premises a computer is seized either for off-site analysis or permanently so requests in writing, the government shall provide to the person within a reasonable time of the request copies of any requested information not subject to permanent seizure (as contraband, fruits of criminal activity, or on other grounds) that may reasonably be necessary or important to the continuing functioning of the person's legitimate activities. If the government withholds any information requested, it shall within a reasonable time of the request identify to the person making the request the information being withheld and the reasons for withholding it.

7. Search Methodology. In conducting the search authorized by this warrant, whether performed on-site or off-site, the government shall make reasonable efforts to utilize a computer search methodology to search for and seize only that information which is identified in the warrant as subject to such search or seizure. The search methodology may include, but is not limited to, the following techniques:



- (a) surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- (b) “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- (c) “scanning” storage areas to discover and possibly recover recently deleted data;
- (d) scanning storage areas for deliberately hidden files; or
- (e) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

8. Unopened Email. Except as expressly provided in the warrant, the warrant and this protocol do not authorize the opening and search of the contents of any kind of unopened electronic mail. In the absence of express authorization in the warrant, no opening and search of unopened electronic mail shall be conducted without a separate search warrant supported by probable cause.

9. Inventories. When a computer has been seized for analysis off-site, the government shall comply with Fed. R. Crim. P. 41(f) in the following manner:

(a) Initial Inventory. Following the on-site search and seizure, the government shall prepare the usual Rule 41(f) inventory of not only the property and items seized by it pursuant to the warrant, but also the information, which has, at that date, been identified as seized pursuant to the warrant. This inventory shall identify each computer that will be subject to further off-site analysis. For example, if the government makes an on-site mirror image of a computer for use in an off-site analysis, the government need only list the making of the mirror image in the return, with an



indication that it is subject to further searching pursuant to this warrant. The listing of any information that is seized from the computer off-site will then be made in the final inventory. The government shall give a copy of the warrant and this initial inventory of property seized to the person from whom or from whose premises the property was taken and make a return to the court, all as provided by Rule 41(f). Because of the nature of electronic or computer information, the listing of seized information in either the initial or final inventory may be made by copying the seized information to a computer diskette, compact disc (*i.e.*, CD), DVD, or like storage device and submitting it along with an affidavit which describes the contents of the storage device.

(b) Final Inventory. After completing the off-site analysis of the computer, the government shall prepare a final inventory of information seized during the off-site analysis. The government shall deliver a copy of the final inventory to the person from whom or from whose premises the computer was taken and make a return of the original final inventory to the court. The court will then attach this final inventory to the original search warrant and initial inventory as an addendum.

10. Copy of Protocol to Searching Personnel. Counsel for the government shall take reasonable steps to ensure that a copy of this protocol is provided to the person or persons who perform the search authorized by this warrant.

11. Superseding Effect. This protocol supersedes any contrary terms set forth in the application for the search warrant, the supporting affidavit, or any attachments thereto.



UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 7/27/09

item(s) listed below were:

- Received From
- Returned To
- Released To
- Seized

(Name) Husen Sherifi

(Street Address) 1320 Steinbeck Drive

(City) Raleigh, N.C.

Description of Item(s): _____

1. HP Pavilion s3709, PC Sn: mxu908003N - Rm B
2. On CD; 5 DVDs - Rm B
3. Paper w/number and writing; airline receipt; DL renewal paper ^{Rm B}
4. Call to Jihad book; Purification of the Soul book - Rm B.
5. VHS tape labeled "Can Democracy Survive the world between Jihad + McWorld" - Rm B
6. 4 VHS tapes - Rm C
7. 14 Books - Rm F
8. 2 Books - Rm B

Nothing to follow

Received By: [Signature]

Received From: none present