FBI File: Twitter, Inc.

Obtained (via FOIA) and posted by AltGov2

www.altgov2.org
Dear Mr. Kick:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed are 97 pages of previously-processed documents and a copy of the Explanation of Exemptions. This release is being provided to you at no charge.

Documents or information referred to other Government agencies were not included in this release.

Please be advised that additional records potentially responsive to your subject may exist. If this release of previously processed material does not satisfy your information needs for the requested subject, you may request an additional search for records. Submit your request by mail or fax to – Work Process Unit, 170 Marcel Drive, Winchester, VA 22602, fax number (540) 868-4997. Please cite the FOIPA Request Number in your correspondence.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP’s FOIAonline portal by creating an account on the following web site: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.
You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state “Dispute Resolution Services.” Please also cite the FOIPA Request Number assigned to your request so that it may be easily identified.

Sincerely yours,

David M. Hardy  
Section Chief,  
Record/Information Dissemination Section  
Records Management Division

Enclosure(s)
EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.
Dear Mr. Kick:

This is in response to your Freedom of Information/Privacy Acts (FOIPA) request. Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

Records regarding your subject were previously reviewed and released to you pursuant to the FOIPA. An additional search was conducted, and no additional records were located. Therefore, your request is being administratively closed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. The “Standard Responses to Requests” section of the Addendum applies to all requests. If the subject of your request is a person, the “Standard Responses to Requests for Individuals” section also applies. The “General Information” section includes useful information about FBI records. Also enclosed is our Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP’s FOIA online portal by creating an account on the following website: https://www.foiaonline.gov/foiaonline/action/public/home. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI’s FOIA Public Liaison by emailing foipaprocesses@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state “Dispute Resolution Services.” Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Sincerely yours,

David M. Hardy
Section Chief,
Record/Information Dissemination Section
Information Management Division

Enclosure
As referenced in our letter, the FBI FOIPA Addendum includes information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. If you submitted a request regarding yourself or another person, Part 2 includes additional standard responses that apply to requests for individuals. If you have questions regarding the standard responses in Parts 1 or 2, visit the www.fbi.gov/foia website under “Contact Us.” Previously mentioned appeal and dispute resolution services are also available. Part 3 includes general information about FBI records that you may find useful.

Part 1: Standard Responses to All Requests: See Below for all Requests

(i) 5 U.S.C. § 552(c). Congress excluded three categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). FBI responses are limited to those records subject to the requirements of the FOIA. Additional information about the FBI and the FOIPA can be found on the fbi.gov website.

(ii) National Security/Intelligence Records. The FBI can neither confirm nor deny the existence of national security and foreign intelligence records pursuant to FOIA exemptions (b)(1) and (b)(3) and PA exemption (j)(2) as applicable to requests for records about individuals [5 U.S.C. §§ 552/552a (b)(1), (b3), and (j)(2); 50 U.S.C § 3024(j)(1)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3); 50 USC § 3024(j)(1). This is a standard response and should not be read to indicate that national security or foreign intelligence records do or do not exist.

Part 2: Standard Responses to Requests for Individuals: See Below for all Requests for Individuals

(i) Requests for Records about any Individual—Watch Lists. The FBI can neither confirm nor deny the existence of any individual’s name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.

(ii) Requests for Records for Incarcerated Individuals. The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E) and (b)(7)(F) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

(i) Record Searches. The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching those systems or locations where responsive records would reasonably be found. Most requests are satisfied by searching the Central Record System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled and maintained by the FBI in the course of fulfilling its dual law enforcement and intelligence mission as well as the performance of agency administrative and personnel functions. The CRS spans the entire FBI organization and encompasses the records of FBI Headquarters (“FBIHQ”), FBI Field Offices, and FBI Legal Attaché Offices (“Legats”) worldwide. A CRS search includes Electronic Surveillance (ELSUR) records.

(ii) FBI Records

Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.

(iii) Requests for Criminal History Records or “Rap Sheets.” The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks—often referred to as a criminal history record or “rap sheet.” These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.

(iv) The National Name Check Program (NNCP). The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private citizens cannot request a name check.
EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FBI/DOJ
UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE       Date: 08/19/2009
To: Cyber                  Attn: SSA
From: San Francisco
     CY-1 / Oakland RA
     Contact: SA

Approved By:                Drafted By: bp

Case ID #: (Pending)

Title: UNSUB(S); TWITTER - VICTIM; COMPUTER INTRUSION - DDOS
       FI BEGIN: 8/13/2009

Synopsis: To initiate a Full Investigation and open a Grand Jury sub-file.

Details: Various news outlets recently reported on Distributed Denial of Service (DDoS) attacks against multiple Bay Area Internet Technology companies including Facebook, LiveJournal, and Twitter. DDoS is a form of Cyber attack in which a large volume of Internet traffic is sent to a targeted computer from multiple sources. The volume of traffic is large enough that it monopolizes the resources of the target causing the target to be unresponsive.

The aforementioned DDoS attacks occurred on August 6, 2009, and caused minimal damages to most targets except Twitter, a company operating a popular online social network of the same name. According to news reports, DDoS attacks against Twitter were directed at a Twitter web page designated to an individual using an online moniker of Cxymu.

On August 13, 2009, FBI San Francisco contacted Twitter, who confirmed the aforementioned attacks. According to reports, the DDoS attacks started on August 6, 2009, at approximately 6:00 am PDT. The attacks consisted of requests from thousands of IP addresses.
requesting a web page located at URL http://www.twitter.com/cyxymu, and made the Twitter web server inaccessible from 6:30 am to 8:30 am. Subsequently, Twitter was again attacked by another DDoS known as a Syn Flood attack. The attack was on-going as of August 13, 2009, but since its initiation, Twitter has been able to bring it to a manageable level.

On Monday, August 11, 2009, starting between 11:30 am and 11:45 am, Twitter experienced a DDoS attack involving User Datagram Protocol (UDP) traffic. The attack lasted approximately 30 minutes. During this time period, Twitter's server received approximately 10 Gigabytes of UDP traffic.

On August 12th and 13th, Twitter was again attacked with floods of UDP traffic. The floods were sporadic and each flood lasted between 1 and 3 minutes.

Based on the facts provided by regarding the aforementioned DDoS attacks against Twitter, SA requests that an investigation be initiated to investigate possible violations of U.S. Code Title 18, Section 1030(5)(1) - intentional transmission of a program or code resulting in damages to a protected computer. The purpose of the investigation is to identify the individual(s) responsible for the aforementioned DDoS attacks.

SA also requests that a Grand Jury sub-file be opened.
LEAD(s):
Set Lead 1: (Info)

CYBER

AT CYBER CRIMINAL SECTION, CCU-2

Read and clear.

♦♦
Incorporated, telephone number [redacted] was telephonically interviewed regarding Distributed Denial of Service (DDoS) attacks against Twitter computer servers. After being advised of the identity of the interviewing and the purpose of the interview, provided the following information:

On August 6, 2009, at approximately 6:00 am PDT, Twitter's web server experienced a DDoS attack consisting of thousands of requests for a web page located at http://www.twitter.com/cyxymu. The attack rendered Twitter's web server inaccessible from 6:30 am to 8:30 am when Twitter was able to fend off the attack with the help of NTT America, a consulting firm, and a Cisco hardware designed to manage DDoS attacks.

Shortly thereafter, Twitter was again attacked by another DDoS known as a Syn Flood attack. On August 9, 2009, NTT America modified Twitter's host-based firewall to fend off the attack. NTT America also applied filters on a peering point located in London to block the traffic of the attack. The London peering point is Twitter's main peering point with Europe, and once filters were applied, the traffic decreased significantly. The attack was ongoing as of August 13, 2009, but since its initiation, Twitter was able to bring it to a manageable level.

On Monday, August 11, 2009, starting between 11:30 am and 11:45 am, Twitter experienced a flood of UDP (User Datagram Protocol) traffic that amounted to approximately 10 Gigabytes. This attack lasted for approximately half an hour.

On August 12th and 13th, Twitter was again attacked with floods of UDP traffic. The floods were sporadic and each flood lasted between 1 and 3 minutes.

Advised that Twitter's web server is located in San Jose, California. All Twitter's servers, including the web server, are managed by NTT America under a contract that existed prior to August 6, 2009. NTT America's assistance in response to the aforementioned DDoS attacks was covered under the contract.
In response to the aforementioned attacks, Twitter also deployed a team of engineers who were on-call 24 hours a day for approximately seven days. All members of the team are salary employees. 

I did not have information regarding losses that may have resulted from the aforementioned attacks and advised that...
Thanks for the information you sent earlier. Based on largely on the lack of cooperation from the victim, we've declined the Twitter case and closed our file.

Regards,

Assistant United States Attorney
United States Attorney's Office
Northern District of California
150 Almaden Blvd. Suite 900
San Jose, CA 95113
tel:
fax: (408) 535-5066
mobile:
On August 13, 2009, FBI San Francisco contacted Twitter, who confirmed the aforementioned attacks. It advised the DDoS attacks started on August 6, 2009, at approximately 6:00 am PDT. The attacks consisted of requests from thousands of IP addresses requesting a web page located at URL http://www.twitter.com/cyxymu. The large number of requests made the Twitter web server inaccessible from 6:30 am to 8:30 am. Subsequently, Twitter was again attacked by another DDoS known as a Syn Flood attack. The attack was on-going as of August 13, 2009, but since its initiation, Twitter has been able to bring it to a manageable level.

On Monday, August 11, 2009, starting between 11:30 am and 11:45 am, Twitter experienced a DDoS attack involving User Datagram Protocol (UDP) traffic. The attack lasted approximately 30 minutes. During this time period, Twitter's server received approximately 10 Gigabytes of UDP traffic.

On August 12th and 13th, Twitter was again attacked with floods of UDP traffic. The floods were sporadic, and each flood lasted between 1 and 3 minutes.

On August 13, 2009, FBI San Francisco initiated an investigation into the aforementioned DDoS attacks.

FBI San Francisco respectfully requests that the U.S. Attorney’s office assign an AUSA to this matter. Questions or comments should be directed to SA at

Sincerely,

Stephanie Douglas
Special Agent in Charge

[Signature]

Supervisory Special Agent
In August 2009, an associate working for NTT America contacted [redacted] and asked for his assistance in fending off DDoS attacks launched against Twitter. [redacted] advised his associate's first name is [redacted] but did not provide the associate's last name. [redacted] agreed to assist [redacted] When [redacted] became involved in fending off the DDoS attacks, approximately twelve hours had already elapsed since the first attack started.

[redacted] and [redacted] identified a botnet involved in the attacks, and the botnet was located within NTT America's network. The identification was made by examining the network traffic and identifying the source IP addresses of the traffic. [redacted] and [redacted] were able to retrieve malware off of one of the bots. By examining the configuration file of the bot, [redacted] was able to determine the identify of the command-and-control server, which was an IRC server. The domain name of the server was [redacted] and it was registered with Dotster. By examining the malware, [redacted] determined that the bot was part of an IRC-based botnet, known as a EnerGyMech botnet. The botnet had a few thousand bots and generated traffic in the hundreds of megabytes. This botnet was small when compared to an average botnet. When [redacted] first identified the command-and-control server, the DNS entry for it had already been removed. Thus, the bots were unable to connect to it.
Precedence: ROUTINE

To: San Francisco

From: San Francisco

Date: 08/25/2010

Contact: SA

Approved By: [Signature]

Drafted By: [Signature]

Case ID #: [Redacted] (Pending) - 5

Title: UNSUB(S);
TWITTER - VICTIM;
COMPUTER INTRUSION - DDOS

Synopsis: To close captioned investigation.

Details: Captioned investigation was initiated on August 24, 2009, in response to a series of Cyber attacks launched against Twitter, a popular social networking website operating out of San Francisco, California. The Cyber attacks began on August 6, 2009, and ended on about August 13, 2009. The Twitter website was rendered inaccessible for approximately two hours due to the Cyber attacks.

NTT America, an Internet Technology consulting company that provides Internet access for the Twitter website, has provided logs of Internet traffic associated with the Cyber attacks against Twitter. However, logs from the Twitter web server, which are under the administration of Twitter, Inc., have not been provided. FBI San Francisco has made multiple requests for the web logs. To date, FBI San Francisco has not received the requested logs.

On July 21, 2010, the United States Attorney's Office (USAO), Northern District of California, notified FBI San Francisco via e-mail stating that it has declined prosecution of the captioned matter due to the lack of cooperation from Twitter. The notification sent by the USAO is attached hereto and incorporated herein.
To: San Francisco  From: San Francisco
Re:  08/25/2010

SA requests that the captioned investigation be closed.

UNCLASSIFIED
In Reply, Please Refer to
File No. ________________

450 Golden Gate Ave.
PO Box 36015
San Francisco, CA 94102
(415) 553-7400
August 25, 2009

Joseph P. Russoniello
United States Attorney
United States Attorney's Office
450 Golden Gate Avenue, 11th Floor
San Francisco, CA 94102

Attention: AUSA

Dear

The purpose of this letter is to request assignment of
an AUSA to assist in an FBI investigation into possible
violations of Title 18, United States Code, section 1030(5)(1) -
intentional transmission of a program or code resulting in
damages to a protected computer.

Various news outlets recently reported on Distributed
Denial of Service (DDoS) attacks against multiple Bay Area
Internet Technology companies including Facebook, LiveJournal,
and Twitter. DDoS is a form of Cyber attack in which a large
volume of Internet traffic is sent to a targeted computer from
multiple sources. The volume of traffic is large enough that it
monopolizes the resources of the target causing the target to be
unresponsive.

The aforementioned DDoS attacks occurred on August 6,
2009, and caused minimal damages to most targets except Twitter,
a company operating a popular online social network of the same
name. According to news reports, DDoS attacks against Twitter
were directed at a Twitter web page designated to an individual
using an online moniker of Cxymu.
FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1341240-0

Total Deleted Page(s) = 6
Page 7 ~ b7E;
Page 11 ~ b7E;
Page 74 ~ b4;
Page 75 ~ b4;
Page 76 ~ b4;
Page 84 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXXX
X  Deleted Page(s)   X
X  No Duplication Fee  X
X  For this Page  X
XXXXXXXXXXXXXXXXXXXXXXXXX
Envelope

Case ID:

1. ORIGINAL NOTES RE INTERVIEW OF [Redacted] SEE SERIAL 2;

2. ORIGINAL NOTES RE INTERVIEW OF [Redacted] SEE SERIAL 4;

3. EMAIL FROM [Redacted] RE LOGS, CD CONTAINING LOGS PROVIDED BY [Redacted] NSLOOKUP RESULTS RE IP’S FOUND IN LOGS, SEE SERIAL 5;
File Number
Field Office Acquiring Evidence: San Francisco
Serial # of Originating Document
Date Received: 8/13/2009
From: Twitter

(Address)

To Be Returned: [ ] Yes [ ] No
Receipt Given: [ ] Yes [ ] No
Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)
Federal Rules of Criminal Procedure: [ ] Yes [ ] No
Federal Taxpayer Information (FTI): [ ] Yes [ ] No

Title:

Reference: FD-302 re interview B

Description: [ ] Original notes re interview of
Aug 6th -

Aug 10th -

London peering point - main peering point to Europe.

Aug 6th - request for URL - Twitter.com/ogyynn

6:28 am 8 & 8:30 am - 100 of thousands

attack blocked

Laser in day Aug 6th.

~ 2000 src IP address SYN flood throughout weekend and morning as of this instant.

probes - new bot addresses - AMP attach type

Mon 11:30am - 11:45 am flood of UDP traffic (~10 gig)

11:45 am - 12:15 pm for ~1/2 an hour

Tues & Wed - spurs of attack by 1st 3 winners

bandwidth - UDP traffic

NTIA - Managed Services
- engaged on W/NITA - turn on device, Cisco
- Host based firewall
  - Modified Sunday

  Money: (out-of-balance & stolen)
  Syn-cookie

  Deception:
  - Gin - Arcester (former law)

  NITA - carries all Tanner traffic
  - will performed as part of contract

  Twitter: 24/7 - 7 days past 3 salted

  - Usually 5-9

  Packet cleaning house - didn't help, no knowledge of it.
FD-340b (Rev. 4-11-03) (A) - (B)

File Number

Field Office Acquiring Evidence San Francisco

Serial # of Originating Document

Date Received 12/09/2009

From

(A)ndrew A. Nettus

(Address)

By

To Be Returned ☐ Yes ☐ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6(e)

Federal Rules of Criminal Procedure ☐ Yes ☐ No

Federal Taxpayer Information (FTI) ☐ Yes ☐ No

Title:

Reference: PD-302 Kre interview

Description: Original notes re-interview of
has an assoc w/ voting for

located a botnet

- Python code loaded on Linux
  webservice
- IRC based botnet
  energy use code based.

Not Black Energy Botnet

- Botnet - a few thousands bot
  somewhat small for a 100s MG
  Botnet

Register to Go Daddy - control
  server

- Don't know who's behind.

- No logs of IPs for bots.
Energy Mech
- Basic command mechanism
- Beacon for lure to web server only
- Connect to IRC server

- LNS''

_ came on alert 12 hrs after attack._

- Arbor
  - build tools to fight DDoS
  - Network tracking
- NCSA
- An Arbor Michigan
Field Office Acquiring Evidence: San Francisco

Date Received: NTT America

Description: Email from [redacted] re current re Coase.

Reference: EC regarding closure of case (Communication Enclosing Material)
Hi

There are two files, the ntt-twitter-attack.tar.gz file contains the logs of the attack against twitter, as well as our infrastructure. The other file is from the initial attack against twitter.

The format for the ntt-eh-* and twitter-* files are:

SRCIP PROTOCOL SRCPORT DSTPORT DATE TIME TZ

The files twitter-20090806.txt and twitter-20090807.txt are standard tcpdump files, but I converted them to plain text.

We don't have logs on this, but this ip, [_____] was found to be attacking Twitter and also contains some very interesting data. I think it may be useful to pursue this.

Let me know if you have any questions!

[_____] is quoted as saying:

> Hi
> > Have you had a chance to compile the logs?
> > Thanks.
> > From: [_____] Sent: Friday, September 11, 2009 1:50 PM
> > To: [_____] Subject: Re: Follow Up Information
> > Hi
> > Sorry for the late response. Friendly timestamp format is preferred.
> > Thanks.
> >
> > ----- Original Message -----
> > From: [_____] Sent: Thu Sep 10 17:58:28 2009
> > To: [_____] Subject: Re: Follow Up Information
> >
> 
>
> Would unix time stamps be okay or would it be easier if I converted them
to a friendlier format?
Domain Dossier  Investigate domains and IP addresses

domain or IP address 128.196.122.199

domain whois record
DNS records
network whois record
traceroute
service scan

user: 65.214.169.254 [anonymous] 49/50

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

lookup failed 128.196.122.199

Could not find a domain name corresponding to this IP address.

Domain Whois record

Don't have a domain name for which to get a record

Network Whois record

Queried whois.arin.net with "128.196.122.199"

OrgName: University of Arizona
OrgID: UOAZ
Address: 1077 N Highland Ave
City: Tucson
StateProv: AZ
PostalCode: 85721
Country: US

NetRange: 128.196.0.0 - 128.196.255.255
CIDR: 128.196.0.0/16
OriginAS: AS1706
NetName: Univ-ARIZ
NetHandle: NET-128-196-0-0-1
Parent: NET-128-0-0-0-0
NetType: Direct Assignment
NameServer: ARIZONA.EDU
NameServer: NS-REMOTE.ARIZONA.EDU
NameServer: OPTIMA.CS.ARIZONA.EDU
NameServer: PENDRAGON.CS.PURDUE.EDU
Comment:
RegDate: 1987-01-22
Updated: 2009-05-18

R: AbuseHandle: ABUSE2144-ARIN
R: AbuseName: Abuse Contact

### Abuse Phone and Email Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abuse Phone</td>
<td>+1-520-626-0100</td>
</tr>
<tr>
<td>Abuse Email</td>
<td><a href="mailto:abuse@arizona.edu">abuse@arizona.edu</a></td>
</tr>
</tbody>
</table>

### Tech Contact Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tech Name</td>
<td></td>
</tr>
<tr>
<td>Tech Phone</td>
<td></td>
</tr>
<tr>
<td>Tech Email</td>
<td></td>
</tr>
</tbody>
</table>

### Organization Abuse Contact Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abuse Name</td>
<td>Abuse Contact</td>
</tr>
<tr>
<td>Abuse Phone</td>
<td>+1-520-626-0100</td>
</tr>
<tr>
<td>Abuse Email</td>
<td><a href="mailto:abuse@arizona.edu">abuse@arizona.edu</a></td>
</tr>
</tbody>
</table>

### Organization Tech Contact Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tech Name</td>
<td></td>
</tr>
<tr>
<td>Tech Phone</td>
<td></td>
</tr>
<tr>
<td>Tech Email</td>
<td></td>
</tr>
</tbody>
</table>

---

# ARIN WHOIS database, last updated 2009-10-03 20:00

## DNS records

DNS query for **199.122.196.128.in-addr.arpa** returned an error from the server: **NameError**

No records to display

---

URL for this output | return to CentralOps.net, a service of Hexillion

---

http://centralops.net/co/DomainDossier.aspx  
10/3/2009
Domain Dossier  Investigate domains and IP addresses

- domain or IP address 193.111.46.169
- domain whois record
- DNS records
- traceroute
- network whois record
- service scan

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name bfawebsite.elsagdatamat.com.

aliases
addresses 193.111.46.169

Domain Whois record

Queried whois.internic.net with "dom elsagdatamat.com"

Domain Name: ELSAGDATAMAT.COM
Registrar: REGISTER.IT SPA
Whois Server: whois.register.it
Referral URL: http://we.register.it
Name Server: DNSA.ELSAGDATAMAT.IT
Name Server: DNSB.ELSAGDATAMAT.IT
Name Server: XGATE.ELSAG.IT
Status: ok
Updated Date: 25-jan-2009
Creation Date: 24-jan-2007
Expiration Date: 24-jan-2010

>>> Last update of whois database: Sun, 04 Oct 2009 03:50:25 UTC <<<

Queried whois.register.it with "elsagdatamat.com"

REGISTER.IT SPA - Whois Server Version 1.4

The Registry database contains ONLY .COM, .NET and .ORG domains.

Domain name: ELSAGDATAMAT.COM
Created on: 2007-01-24
Updated on: 2009-02-18
Expires on: 2010-01-24
Registrant Name: KEYCAB SPA
Contact: KEYCAB SPA
Registrant Address: VIA
Registrant City: ROMA

Registrant Postal Code: 00143
Registrant Country: IT
Administrative Contact Organization: Register.it S.p.A.
Administrative Contact Name: MM2172-RIPE
Administrative Contact Address: Via Montessori s/n
Administrative Contact City: Bergamo
Administrative Contact Postal Code: 24126
Administrative Contact Country: IT
Administrative Contact Email: support@register.it
Administrative Contact Phone: +39 035 3230400
Administrative Contact Fax: +39 035 3230312
Primary Name Server Hostname: DNSA.ELSAGDATAMAT.IT
Secondary Name Server Hostname: DNSSB.ELSAGDATAMAT.IT

>>> Last update of whois database: Sun Oct 4 03:55:49 2009 <<<

Network Whois record

Queried whois.ripe.net with "-B 193.111.46.169"...

% Information related to '193.111.46.0 - 193.111.46.255'
inetnum: 193.111.46.0 - 193.111.46.255
netname: KEYCAB-NET
descr: KeyCab S.p.A
country: IT
admin-c: CN148-RIPE
tech-c: MM2172-RIPE
status: ASSIGNED PI
mnt-by: RIPE-NCC-HM-PI-MNT
mnt-lower: RIPE-NCC-HM-PI-MNT
mnt-by: INET-NOC
mnt-routes: INET-NOC
changed: hostmaster@ripe.net 20020318
source: RIPE

person: hostmaster@ripe.net 20020318
address: 
phone: 
fax-no: 
notify: network@keycab.com
nic-hdl: CN148-RIPE
changed: hostmaster@ripe.net 20020318
source: RIPE

phone: network@keycab.com
fax-no: 
notify: network@keycab.com
nic-hdl: MM2172-RIPE
changed: hostmaster@ripe.net 20020318
source: RIPE

% Information related to '193.111.46.0/24AS24802'

route: 193.111.46.0/24
descr: KEYCAB-NET
origin: AS24802
notify: noc@inet.it
mnt-by: INET-NOC
changed: RIPE
source: RIPE

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfawebbsite.elsagdatamat.com</td>
<td>IN</td>
<td>A</td>
<td>193.111.46.169</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>SOA</td>
<td>server: dnsa.elsagdatamat.it, email: hostmaster.elsagdatamat.com, serial: 1253169426, refresh: 16384, retry: 2048, expire: 1048576, minimum ttl: 2560</td>
<td>2560s (00:42</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>NS</td>
<td>dnsa.elsagdatamat.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>NS</td>
<td>dnsb.elsagdatamat.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>NS</td>
<td>xgate.elsag.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10, exchange: elcgepulmxlb.elsag.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 400, exchange: elcgepulmx01.elsag.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 400, exchange: elcgepulmx02.elsag.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 400, exchange: elcgepulmx03.elsag.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>elsagdatamat.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 400, exchange: elcgepulmx04.elsag.it</td>
<td>86400s (1.00:</td>
</tr>
<tr>
<td>169.46.111.193.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>bfawebbsite.elsagdatamat.com</td>
<td>86400s (1.00:</td>
</tr>
</tbody>
</table>

-- end --

Domain Dossier  Investigate domains and IP addresses

domain or IP address  193.142.215.38

☑ domain whois record  ☑ DNS records  ☐ traceroute
☑ network whois record  ☐ service scan  

user: 65.214.169.254 [anonymous] 47/50
log in | get account

centralOps.net

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

lookup failed  193.142.215.38

Could not find a domain name corresponding to this IP address.

Domain Whois record

Don't have a domain name for which to get a record

Network Whois record

Queried whois.ripe.net with "-B 193.142.215.38"

% Information related to '193.142.215.0 - 193.142.215.255'

netname: NL-CITUS
descr: Citus internetdiensten
country: NL

org: ORG-Ci24-RIPE
admin-c: DARS1-RIPE
tech-c: DARS1-RIPE
status: ASSIGNED PI
notify: noc@grafix.nl
mnt-by: RIPE-NCC-HM-PI-MNT
mnt-by: GFX-MNT
mnt-lower: RIPE-NCC-HM-PI-MNT
mnt-routes: GFX-MNT
mnt-domains: GFX-MNT
changed: noc@grafix.nl 20070329
source: RIPENCC

organisation: ORG-Ci24-RIPE
org-name: Citus internetdiensten
org-type: OTHER
address: Hondelink 61
address: 7482 KP Haaksbergen
address: The Netherlands

% Information related to '193.142.215.0/24AS16131'

route: 193.142.215.0/24
descr: Citus internetdiensten
origin: AS16131
mnt-by: GFX-MNT
changed: noc@grafix.nl 20070323
source: RIPE

DNS records

DNS query for 38.215.142.193.in-addr.arpa returned an error from the server: NameError

No records to display
Domain Dossier  Investigate domains and IP addresses

domain or IP address: 193.16.154.115

- domain whois record
- DNS records
- network whois record
- traceroute

user: 65.214.169.254 [anonymous] 46/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name: ded104.zylon.net.
aliases
addresses: 193.16.154.115

Domain Whois record

Queried whois.internic.net with "dom zylon.net"...

Domain Name: ZYLON.NET
Registrar: ENOM, INC.
Whois Server: whois.enom.com
Referral URL: http://www.enom.com
Name Server: A.NS.ZYLON.NET
Name Server: B.NS.ZYLON.NET
Status: clientTransferProhibited
Updated Date: 28-sep-2009
Creation Date: 27-oct-2001
Expiration Date: 27-oct-2010

Last update of whois database: Sun, 04 Oct 2009 03:52:13 UTC

Queried whois.enom.com with "zylon.net"

Registration Service Provided By: Enom, Inc
Contact: CustomerSupport@enom.com
Visit: www.enom.com

Domain name: zylon.net
Registrant Contact:

Zylon
Fax:

http://centralops.net/co/DomainDossier.aspx

10/3/2009
Administrative Contact:
Zylon Internet Services
Fax:

Technical Contact:
Zylon Internet Services
Fax:

Status: Locked

Name Servers:
a.ns.zylon.net
b.ns.zylon.net

Expiration date: 27 Oct 2010 22:27:00

Get Noticed on the Internet! Increase visibility for this domain name by listing it at

Network Whois record

Queried whois.ripe.net with "-B 193.16.154.115"

% Information related to '193.16.154.0 - 193.16.154.255'

inetnum: 193.16.154.0 - 193.16.154.255
netname: NL-ZYLON
descr: Webhost/colocation
country: NL
org: ORG-ZYLO1-RIPE
admin-c: ES2004-ripe
tech-c: ES2004-ripe
status: ASSIGNED PI
notify:
mnt-by: RIPE-NCC-HM-PI-MNT
mnt-by: ZYLON-NOC
mnt-lower: RIPE-NCC-HM-PI-MNT
mnt-routes: ZYLON-NOC
mnt-domains: ZYLON-NOC
changed:
source: RIPE
organisation: ORG-ZYLO1-RIPE
org-name: Zylon Internet Services
org-type: OTHER
address: Protonstraat 6c
address: 9743AL Groningen
address: The Netherlands
e-mail: noc@zylon.net
mnt-ref: ZYLON-NOC
mnt-by: ZYLON-NOC
changed: hostmaster@zylon.net 20080814
source: RIPE

person: 
address: 
address: 
address: 
phone: 
fax-no: 
nic-hdl: ES2004-ripe
mnt-by: ZYLON-NOC
e-mail: hostmaster@zylon.net
notify: hostmaster@zylon.net
changed: hostmaster@zylon.net 20080814
source: RIPE

% Information related to '193.16.154.0/24AS8312'
route: 193.16.154.0/24
descr: Zylon webhosting
origin: AS8312
notify: noc@zylon.net
mnt-by: ZYLON-NOC
changed: iomnt@io.nl 20040525
source: RIPE

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>ded104.zylon.net</td>
<td>IN</td>
<td>A</td>
<td>193.16.154.40</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>zylon.net</td>
<td>IN</td>
<td>MX</td>
<td>preference:</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: scrubber1.as8312.net</td>
<td></td>
</tr>
<tr>
<td>zylon.net</td>
<td>IN</td>
<td>NS</td>
<td>a.ns.zylon.net</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>zylon.net</td>
<td>IN</td>
<td>NS</td>
<td>b.ns.zylon.net</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>zylon.net</td>
<td>IN</td>
<td>A</td>
<td>193.16.154.40</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>zylon.net</td>
<td>IN</td>
<td>SOA</td>
<td>server: a.ns.zylon.net</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email: hostmaster.zylon.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 2004012700</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 10800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 3600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 604800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 3600</td>
<td></td>
</tr>
<tr>
<td>115.154.16.193.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>ded104.zylon.net</td>
<td>3600s (01:00:00)</td>
</tr>
</tbody>
</table>

http://centralops.net/co/DomainDossier.aspx

10/3/2009
Domain Dossier  Investigate domains and IP addresses

- domain or IP address: 193.19.92.164
- ✔ domain whois record
- ✔ DNS records
- ✔ network whois record
- ✔ traceroute
- ✔ service scan

user: 65.214.169.254 [anonymous] 45/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup


aliases

domain addresses: 193.19.92.164

Domain Whois record

Queried whois.internic.net with "dom hanival.com"...

Domain Name: HANIVAL.COM
Registrar: DIRECTI INTERNET SOLUTIONS PVT. LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Whois Server: whois.PublicDomainRegistry.com
Referral URL: http://www.PublicDomainRegistry.com
Name Server: NS1.HANIVAL.COM
Name Server: NS2.HANIVAL.COM
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 25-feb-2009
Creation Date: 01-mar-2005
Expiration Date: 01-mar-2011

Last update of whois database: Sun, 04 Oct 2009 03:53:45 UTC

Queried whois.publicdomainregistry.com with "hanival.com"...

Registration Service Provided By: CHILLYDOMAINS
Contact: +43.13195843

Domain Name: HANIVAL.COM

Registrant:
  Hanival Internet Services GmbH
  Hanival Domainadmin (office@hanival.net)
  Kirchengasse 13/1a
  Wien
  null,1070

AT
Tel. +43.13195843
Fax. +43.1319584324

Creation Date: 01-Mar-2005
Expiration Date: 01-Mar-2011

Domain servers in listed order:
ns1.hanival.com
ns2.hanival.com

Administrative Contact:
Hanival Internet Services GmbH
Hanival Domainadmin (office@hanival.net)
Kirchengasse 13/1a
Wien
null,1070
AT
Tel. +43.13195843
Fax. +43.1319584324

Technical Contact:
Hanival Internet Services GmbH
Hanival Domainadmin (office@hanival.net)
Kirchengasse 13/1a
Wien
null,1070
AT
Tel. +43.13195843
Fax. +43.1319584324

Billing Contact:
Hanival Internet Services GmbH
Hanival Domainadmin (office@hanival.net)
Kirchengasse 13/1a
Wien
null,1070
AT
Tel. +43.13195843
Fax. +43.1319584324

Status: LOCKED
Note: This Domain Name is currently Locked. In this status the domain name cannot be transferred, hijacked, or modified. The Owner of this domain name can easily change this status from their control panel. This feature is provided as a security measure against fraudulent domain name.

Network Whois record
Queried whois.ripe.net with "-B 193.19.92.164"

% Information related to '193.19.92.0 - 193.19.93.255'
netname: HANIVAL-NET
descr: Hanival Internet Services GmbH
descr: hanival.com Infrastructure Vienna
country: AT
<table>
<thead>
<tr>
<th>Role</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hanival Hostmaster</td>
<td>Hostmaster Role for Hanival</td>
</tr>
</tbody>
</table>

**Organisation:** ORG-HAN1-RIPE

**Domain:** Hanival Internet Services GmbH

**Address:** Kirchengasse 13/1a, A-1070, Vienna, Austria

**E-mail:** hostmaster@hanival.com

**MNT-Ref:** MNT-HANIVAL

**Source:** RIPE

**Person:**

<table>
<thead>
<tr>
<th>Address</th>
<th>Phone</th>
<th>E-mail</th>
<th>NIC-HDL</th>
<th>MNT-Ref</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>GH1975-RIPE</td>
<td>MNT-REBEL-SYSTEMS</td>
<td>RIPE</td>
</tr>
</tbody>
</table>

**Changed:**

- Hostmaster@ripe.net 20071207
- Hostmaster@ripe.net 20071210

http://centralops.net/co/DomainDossier.aspx

10/3/2009
source: RIPE

% Information related to '193.19.92.0/23AS44904'

route: 193.19.92.0/23
descr: Hanival Internet Services GmbH
origin: AS44904
mnt-by: MNT-HANIVAL
changed: RIPE

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>crm-staging.hanival.com</td>
<td>IN</td>
<td>A</td>
<td>193.19.92.164</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>hanival.com</td>
<td>IN</td>
<td>SOA</td>
<td>server: ns1.hanival.com</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email: hostmaster.hanival.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 2009051401</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 10800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 3600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 3600000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 360000</td>
<td></td>
</tr>
<tr>
<td>hanival.com</td>
<td>IN</td>
<td>NS</td>
<td>ns2.hanival.com</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>hanival.com</td>
<td>IN</td>
<td>NS</td>
<td>ns1.hanival.com</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>hanival.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail.hanival.com</td>
<td></td>
</tr>
<tr>
<td>hanival.com</td>
<td>IN</td>
<td>A</td>
<td>80.252.37.230</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>164.92.19.193.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>crm-staging.hanival.com</td>
<td>298s (00:04:58)</td>
</tr>
</tbody>
</table>

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier  Investigate domains and IP addresses

- domain or IP address: 193.24.208.11
- domain whois record
- DNS records
- network whois record
- traceroute
- service scan

user: 65.214.169.254 [anonymous] 44/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

lookup failed 193.24.208.11

Could not find a domain name corresponding to this IP address.

Domain Whois record

Don't have a domain name for which to get a record

Network Whois record

Queried whois.ripe.net with "-B 193.24.208.11"

* Information related to '193.24.208.0 - 193.24.211.255'

inetnum: 193.24.208.0 - 193.24.211.255
netname: ISP4P-NET
mnt-lower: Link1-MNT
mnt-routes: Link1-MNT
mnt-by: Link1-MNT
descr: ISP4P EDV IT Services
country: DE
admin-c: OD250-RIPE
tech-c: OD250-RIPE
status: ASSIGNED PI
mnt-by: ISP4P-MNT
mnt-by: RIPE-NCC-HM-PI-MNT
mnt-lower: RIPE-NCC-HM-PI-MNT
mnt-routes: ISP4P-MNT
mnt-domains: ISP4P-MNT
changed: hostmaster@ripe.net 20060210
source: RIPE

g3

person:
address:

b6
b7C

% Information related to '193.24.208.0/22AS35042'

route: 193.24.208.0/22
desc: ISP4P Network
origin: AS35042
mnt-by: ISP4P-MNT
changed: hostmaster@isp4p.net 20050526
source: RIPE

% Information related to '193.24.208.0/22AS41003'

route: 193.24.208.0/22
desc: AS41003
origin: AS41003
mnt-by: ISP4P-MNT
changed: hostmaster@isp4p.net 20070429
source: RIPE

DNS records

DNS query for 11.208.24.193.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier  Investigate domains and IP addresses

domain or IP address  195.248.255.138

☑ domain whois record  ☑ DNS records  ☑ traceroute
☑ network whois record  ☑ service scan

user: 65.214.169.254 [anonymous] 43/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

lookup failed 195.248.255.138

Could not find a domain name corresponding to this IP address.

Domain Whois record

Don't have a domain name for which to get a record

Network Whois record

Queried whois.ripe.net with "-B 195.248.255.138"

% Information related to '195.248.254.0 - 195.248.255.255'

inetnum: 195.248.254.0 - 195.248.255.255
netname: TRANS-NET-TYCHY-PL
descr: Trans-Net
country: PL
org: ORG-TA263-RIPE
admin-c: MG9821-RIPE
tech-c: MG9821-RIPE
status: ASSIGNED PI
mnt-by: IPARTNERS-MNT
mnt-by: TRANS-NET-MNT
mnt-by: RIPE-NCC-HM-PI-MNT
mnt-domains: IPARTNERS-MNT
mnt-domains: TRANS-NET-MNT
mnt-lower: RIPE-NCC-HM-PI-MNT
mnt-routes: IPARTNERS-MNT
mnt-routes: TRANS-NET-MNT
changed: hostmaster@ripe.net 20070330
source: RIPE

organisation: ORG-TA263-RIPE
org-name: Trans-Net
org-type: OTHER
address: ul. Mikolowska 99

195.248.255.138 - Domain Dossier - owner and registrar information, whois and DNS rec...

address: 43-100 Tychy
address: Poland
phone: 
e-mail: 
admin-c: MG9821-RIPE
technical-c: MG9821-RIPE
mnt-ref: IPARTNERS-MNT
mnt-by: IPARTNERS-MNT
changed: 
source: RIPE

person: 
address: 
e-mail: 
phone: 
fax-no: 
notify: 
mnt-by: IPARTNERS-MNT
nic-hdl: MG9821-RIPE
changed: 
source: RIPE

% Information related to '195.248.254.0/23 AS42717'

route: 195.248.254.0/23
descr: Trans-Net ISP
origin: AS42717
mnt-by: TRANS-NET-MNT
mnt-lower: TRANS-NET-MNT
remarks: for spam/abuse complaints: abuse@trans.net.pl
changed: 
source: RIPE

DNS records

DNS query for 138.255.248.195.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

Domain Dossier  Investigate domains and IP addresses

- Domain or IP address: 195.28.22.35
- Domain WHOIS record
- DNS records
- Network WHOIS record
- Service scan

**New:** Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

- Canonical name: w22035.exception.nl
- Aliases
- Addresses: 195.28.22.35

Domain Whois record

Queried whois.domain-registry.nl with "exception.nl"...

- Domain name: exception.nl
- Status: active
- Registrant: Exception IT Services
  Helperpark 298 A
  9723ZA GRONINGEN
  Netherlands
  Administrative contact:
  GRO015586-EXCEP
  postmaster@exception.nl
- Registrar: Exception IT Services
  Helperpark 298 A
  9723ZA GRONINGEN
  Netherlands
- Technical contact(s):
  KOE005602-EXCEP
  admin@exception.nl

Domain nameservers:
nsx1.exception.nl  195.28.22.6
nsx2.exception.nl  195.28.22.5

Date registered: 07-03-2000
Record last updated: 30-03-2009
Record maintained by: NL Domain Registry

Network Whois record

Queried whois.ripe.net with "-B 195.28.22.35"...

% Information related to '195.28.22.0 - 195.28.23.255'

inetnum:      195.28.22.0 - 195.28.23.255
netname:      EXCEPTION-CUSTOMER-OSSO
descr:        Exception IT services
country:      NL
org:          ORG-EIs9-RIPE
admin-c:      MG11512-RIPE
tech-c:       MG11512-RIPE
status:       ASSIGNED PI
notify:       noc@osso.nl
mnt-by:       RIPE-NCC-END-MNT
mnt-by:       MNT-OSSOBV
mnt-lower:    RIPE-NCC-END-MNT
mnt-routes:   MNT-OSSOBV
mnt-domains:  MNT-OSSOBV
changed:      hostmaster@ripe.net 20090320
source:       RIPE

organisation: ORG-EIs9-RIPE
org-name:     Exception IT services
admin-c:      MG11512-RIPE
tech-c:       MG11512-RIPE
org-type:     OTHER
address:      

e-mail:       info@exception.nl
mnt-ref:      MNT-OSSOBV
mnt-by:       MNT-OSSOBV
changed:      noc@osso.nl 20090317
source:       RIPE

person:       
address:      

mnt-by:       MNT-OSSOBV
phone:        
fax-no:       
org:          ORG-EIs9-RIPE
nic-hdl:      MG11512-RIPE
changed:      noc@osso.nl 20090317
source:       RIPE

% Information related to '195.28.22.0/24AS43366'

route: 195.28.22.0/24
descr: Exception subnet1
mnt-by: MNT-DUOCAST
origin: AS43366
mnt-by: MNT-OSSOBV
changed: noc@osso.nl 20090320
source: RIPE

% Information related to '195.28.22.0/24AS43113'
route: 195.28.22.0/24
descr: Exception subnetl
mnt-by: MNT-DUOCAST
origin: AS43113
mnt-by: MNT-OSSOBV
changed: noc@osso.nl 20090320
changed: f.labohm@duocast.nl 20090325
source: RIPE

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>w22035.exception.nl</td>
<td>IN</td>
<td>A</td>
<td>195.28.22.35</td>
<td>28800s (08:00:00)</td>
</tr>
<tr>
<td>exception.nl</td>
<td>IN</td>
<td>A</td>
<td>195.28.22.31</td>
<td>28800s (08:00:00)</td>
</tr>
<tr>
<td>exception.nl</td>
<td>IN</td>
<td>SOA</td>
<td>nsx1.exception.nl</td>
<td>28800s (08:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>admin.exception.nl</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 2009092504</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 21600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 7200</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 604800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 28800</td>
<td></td>
</tr>
<tr>
<td>exception.nl</td>
<td>IN</td>
<td>NS</td>
<td>nsx1.exception.nl</td>
<td>28800s (08:00:00)</td>
</tr>
<tr>
<td>exception.nl</td>
<td>IN</td>
<td>NS</td>
<td>nsx2.exception.nl</td>
<td>28800s (08:00:00)</td>
</tr>
<tr>
<td>exception.nl</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>28800s (08:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail1.exception.nl</td>
<td></td>
</tr>
<tr>
<td>exception.nl</td>
<td>IN</td>
<td>MX</td>
<td>preference: 20</td>
<td>28800s (08:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail2.exception.nl</td>
<td></td>
</tr>
<tr>
<td>35.22.28.195.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>w22035.exception.nl</td>
<td>28798s (07:59:58)</td>
</tr>
</tbody>
</table>

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

http://centralops.net/co/DomainDossier.aspx
Domain Dossier  Investigate domains and IP addresses

domain or IP address 195.34.184.98

✔ domain whois record ✔ DNS records     ❏ traceroute

✔ network whois record     ❏ service scan (99)

user: 65.214.169.254 [anonymous] 41/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name internic.de.

aliases
addresses 195.34.184.98

Domain Whois record

Queried whois.denic.de with "-T new,ace,dn -C UTF-8 internic.de"...

Domain: internic.de
Domain-Ace: internic.de
Nservers: ns.ger.fra.ivs.de
Nservers: ns.ger.bln.ivs.de
Nservers: ns.ger.stg.ivs.de
Status: connect
Changed: 2008-11-21T13:13:54+01:00

[Tech-C]
Type: PERSON
Name: Hostmaster INTERNIC
Address: Wiesenhuettenplatz 26
Pcode: 60329
City: Frankfurt
Country: DE
Phone: +49-69-272340
Fax: +49-69-27234444
Email: denic@internic.de
Changed: 2006-12-13T13:15:28+01:00

[Zone-C]
Type: PERSON
Name: Hostmaster INTERNIC
Address: Wiesenhuettenplatz 26
Pcode: 60329
City: Frankfurt
Country: DE
Phone: +49-69-272340
Fax: +49-69-27234444
Network Whois record

Queried whois.ripe.net with "-B 195.34.184.98"

% Information related to '195.34.160.0 - 195.34.191.255'

inetnum: 195.34.160.0 - 195.34.191.255
org: ORG-IG36-RIPE
netname: DE-NIC-971014
descr: INTERNIC GmbH
country: DE
admin-c: AS43-RIPE
tech-c: HIS4-RIPE
tech-c: STS30-RIPE
tech-c: STS
status: Allocated PA
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: MNT-INTERNIC
mnt-routes: MNT-INTERNIC
mnt-domains: MNT-INTERNIC
changed: hostmaster@ripe.net 19971014
changed: hostmaster@ripe.net 20000605
changed: hostmaster@ripe.net 20060217
changed: bitbucket@ripe.net 20080714
source: RIPE

organisation: ORG-IG36-RIPE
org-name: INTERNIC GmbH
org-type: LIR
address: INTERNIC GmbH

phone:
fax-no:
e-mail:
admin-c: CPS1-RIPE
admin-c: STS30-RIPE
admin-c: AS43-RIPE
mnt-ref: RIPE-NCC-HM-MNT
mnt-ref: MNT-INTERNIC
mnt-by: RIPE-NCC-HM-MNT
changed: hostmaster@ripe.net 20060106
changed: bitbucket@ripe.net 20060110
changed: hostmaster@ripe.net 20060111
changed: bitbucket@ripe.net 20060111
changed: bitbucket@ripe.net 20060112
changed: bitbucket@ripe.net 20060131
changed: bitbucket@ripe.net 20060208
changed: bitbucket@ripe.net 20060209
changed: bitbucket@ripe.net 20060209
changed: bitbucket@ripe.net 20060210
changed: bitbucket@ripe.net 20060217
changed: bitbucket@ripe.net 20060217
changed: bitbucket@ripe.net 20060313
changed: bitbucket@ripe.net 20060419
changed: bitbucket@ripe.net 20060524
changed: bitbucket@ripe.net 20060524
changed: bitbucket@ripe.net 20060524
changed: bitbucket@ripe.net 20060524
changed: bitbucket@ripe.net 20060524
changed: bitbucket@ripe.net 20070302
changed: bitbucket@ripe.net 20070312
changed: bitbucket@ripe.net 20070813
changed: bitbucket@ripe.net 20070829
source: RIPE

person: c/o INTERNIC GmbH
address: INTERNIC GmbH ex DeBONE
address: INTERNIC GmbH
address: INTERNIC GmbH
phone: 
fax-no: 
e-mail: 
nic-hdl: AS43-RIPE
mnt-by: INTERNET-NOC
mnt-by: MNT-INTERNIC
changed: hostmaster@inet.de 19990718
changed: 
source: RIPE

person: Hostmaster INTERNET
address: INTERNIC GmbH ex DeBONE
address: INTERNIC GmbH
address: INTERNIC GmbH
phone: 
fax-no: 
e-mail: 
e-mail: 
nic-hdl: HIS4-RIPE
remarks: Hostmaster of the day
notify: INTERNET-NOC
mnt-by: 
changed: hostmaster@inet.de 19990209
changed: 
changed: 
source: RIPE

person: 
address: INTERNIC GmbH
address: INTERNIC GmbH
address: INTERNIC GmbH
mnt-by: MNT-INTERNIC
phone: 
fax-no: 
e-mail: 
nic-hdl: STS30-RIPE
changed: 
source: RIPE

person: 
address: INTERNIC GmbH
address: INTERNIC GmbH
address: INTERNIC GmbH

address: 
phone:  
fax-no: 
e-mail: support@internic.de
nic-hdl: STS
changed: support@internic.de 20060625
mnt-by: INTERNIC
mnt-by: MNT-INTERNIC
source: RIPE

% Information related to '195.34.160.0/19AS8495'

route: 195.34.160.0/19
descr: INTERNIC GmbH
origin: AS8495
mnt-by: MNT-INTERNIC
changed:  
changed:  
changed:  
source: RIPE

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>internic.de</td>
<td>IN</td>
<td>A</td>
<td>195.34.168.99</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>internic.de</td>
<td>IN</td>
<td>NS</td>
<td>ns.ger.bln.ivs.de</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>internic.de</td>
<td>IN</td>
<td>NS</td>
<td>ns.ger.stg.ivs.de</td>
<td>10800s (03:00:00)</td>
</tr>
<tr>
<td>internic.de</td>
<td>IN</td>
<td>SOA</td>
<td>ns.ger.fra.ivs.de</td>
<td>10800s (03:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>hostmaster.ivs.de</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh:</td>
<td>2009072801</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry:</td>
<td>7200</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire:</td>
<td>604800</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl:</td>
<td>10800</td>
</tr>
<tr>
<td>internic.de</td>
<td>IN</td>
<td>NS</td>
<td>ns.ger.fra.ivs.de</td>
<td>10800s (03:00:00)</td>
</tr>
<tr>
<td>internic.de</td>
<td>IN</td>
<td>MX</td>
<td>preference:</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange:</td>
<td>mx.inet.de</td>
</tr>
<tr>
<td>internic.de</td>
<td>IN</td>
<td>MX</td>
<td>preference:</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange:</td>
<td>mx2.inet.de</td>
</tr>
<tr>
<td>98.184.34.195.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>internic.de</td>
<td>43200s (12:00:00)</td>
</tr>
</tbody>
</table>

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier - Investigate domains and IP addresses

- Domain Dossier
- Investigate domains and IP addresses
- domain or IP address: 195.4.3.87
- ✔ domain whois record
- ✔ DNS records
- ✔ network whois record
- ✔ traceroute
- ✔ service scan

Log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name: 10.moenchengladbach01.fdknet.de.

aliases: 
addresses: 195.4.3.87

Domain Whois record

Queried whois.denic.de with "-T new,ace,dn -C UTF-8 fdknet.de"...

Domain: fdknet.de
Domain-Ace: fdknet.de
Nserver: dns.roka.net
Nserver: metallica.roka.de
Nserver: ns1.freenet.de
Nserver: ns1.free-net.net
Status: connect
Changed: 2007-07-19T13:36:12+02:00

[Tech-C]
Type: ROLE
Name: Domain Registration Role-Account
Address: freenet Datenkommunikations GmbH
Address: Willstaetterstr. 13
Pcode: 40549
City: Duesseldorf
Country: DE
Phone: +49 211 53087 0
Fax: +49 211 53087 199
Email: domreg@roka.net
Changed: 2009-01-21T09:56:06+01:00

[Zone-C]
Type: ROLE
Name: Domain Registration Role-Account
Address: freenet Datenkommunikations GmbH
Address: Willstaetterstr. 13
Pcode: 40549
City: Duesseldorf
Country: DE
Phone: +49 211 53087 0
Fax: +49 211 53087 199
Email: domreg@roka.net
Changed: 2009-01-21T09:56:06+01:00

Network Whois record
Queried whois.ripe.net with "-B 195.4.3.87"

% Information related to '195.4.3.87 - 195.4.3.87'
inetnum: 195.4.3.87 - 195.4.3.87
netname: IMPRESS-MEDIA-NET
descr: impress media GmbH
country: DE
admin-c: SadHl-RIPE
tech-c: FCL-RIPE
status: ASSIGNED PA
mnt-by: ROKA-MNT
changed: tech-c@mcbone.net 20070713
source: RIPE

role: freenet Cityline Network Management
address: freenet Cityline GmbH
address: Am Germaniahafen 1-7
address: 24143 Kiel
address: Germany
e-mail: tech-c@mcbone.net
abuse-mailbox: abuse@pppool.de
admin-c: FCL-RIPE
tech-c: JR1741-RIPE
tech-c: KR2D
tech-c: SH-RIPE
tech-c: SW817-RIPE
nic-hdl: FCL-RIPE
mnt-by: ROKA-MNT
changed: abuse@pppool.de 20071010
source: RIPE

person: impress media GmbH
address: impress media GmbH
phone: abuse@mcbone.net
nic-hdl: SadHl-RIPE
mnt-by: ROKA-P
changed: abuse@mcbone.net 20070713
source: RIPE

% Information related to '195.4.0.0/16AS5430'
route: 195.4.0.0/16
descr: freenet Cityline GmbH
descr: Am Germaniahafen 1-7

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>I0.moenchengladbach01.fdknet.de</td>
<td>IN</td>
<td>A</td>
<td>195.4.3.87</td>
<td>86400s (1.00:0C)</td>
</tr>
<tr>
<td>fdknet.de</td>
<td>IN</td>
<td>NS</td>
<td>ns1.free-net.net</td>
<td>86400s (1.00:0C)</td>
</tr>
<tr>
<td>fdknet.de</td>
<td>IN</td>
<td>NS</td>
<td>ns1.freenet.de</td>
<td>86400s (1.00:0C)</td>
</tr>
<tr>
<td>fdknet.de</td>
<td>IN</td>
<td>SOA</td>
<td>server: ns1.freenet.de, email: hostmaster.roka.net, serial: 2008012032, refresh: 86400, retry: 7200, expire: 2419200, minimum ttl: 3600</td>
<td>86400s (1.00:0C)</td>
</tr>
<tr>
<td>fdknet.de</td>
<td>IN</td>
<td>NS</td>
<td>metallica.roka.de</td>
<td>86400s (1.00:0C)</td>
</tr>
<tr>
<td>fdknet.de</td>
<td>IN</td>
<td>A</td>
<td>194.97.8.18</td>
<td>300s (00:05:01)</td>
</tr>
<tr>
<td>fdknet.de</td>
<td>IN</td>
<td>MX</td>
<td>preference: 5</td>
<td>86400s (1.00:0C)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mx.freenet.de</td>
<td></td>
</tr>
<tr>
<td>fdknet.de</td>
<td>IN</td>
<td>NS</td>
<td>dns.roka.net</td>
<td>86400s (1.00:0C)</td>
</tr>
<tr>
<td>87.3.4.195.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>I0.moenchengladbach01.fdknet.de</td>
<td>86400s (1.00:0C)</td>
</tr>
</tbody>
</table>
Domain Dossier  Investigate domains and IP addresses

- domain whois record
- DNS records
- network whois record
- traceroute
- service scan

log in | get account

canonical name i2arl.motlabs.com.
aliases
addresses 199.104.137.69

Domain Whois record

Queried whois.internic.net with "dom motlabs.com"

Domain Name: MOTLABS.COM
Registrar: CSC CORPORATE DOMAINS, INC.
Whois Server: whois.corporatedomains.com
Referral URL: http://www.cscprotectsbrands.com
Name Server: DNS1.MOTLABS.COM
Name Server: DNS2.MOTLABS.COM
Status: clientTransferProhibited
Updated Date: 22-apr-2009
Creation Date: 26-apr-1999
Expiration Date: 26-apr-2010

>>> Last update of whois database: Sun, 04 Oct 2009 04:10:54 UTC <<<

Queried whois.corporatedomains.com with "motlabs.com"

Corporation Service Company(c) (CSC) The Trusted Partner of More than 50% of the 100 E
Contact us to learn more about our enterprise solutions for Global Domain Name Regist
NOTICE: You are not authorized to access or query our WHOIS database through the use of

Registrant:
Motorola, Inc.
Domain Admin
1303 E. Algonquin Road
Schaumburg, IL 60196
US
Email: internic@motorola.com

Registrar Name: CORPORATE DOMAINS, INC.
Registrar WHOIS: whois.corporatedomains.com
Registrar Homepage: www.cscprotectsbrands.com

Domain Name: motlabs.com

Created on: Mon, Apr 26, 1999
Expires on: Mon, Apr 26, 2010
Record last updated on: Wed, Apr 22, 2009

Administrative Contact:
Motorola, Inc.
Domain Admin
1303 E. Algonquin Road
Schaumburg, IL 60196
US
Phone: 001-847-5765000
Email: internic@motorola.com

Technical Contact:
Register.Com
Registrar Internic
575 8th Avenue
New York, NY 10018
US
Phone: 001-212-5949880
Email: internic-free@register.com

DNS Servers:
dns1.motlabs.com
dns2.motlabs.com

Register your domain name at http://www.cscprotectsbrands.com

Network WHOIS record

Queried whois.arin.net with "!NET-199-104-128-0-2"

OrgName: Motorola SPS
OrgID: MOTORO-7
Address: 2100 East Elliot Road
City: Tempe
StateProv: AZ
PostalCode: 85284
Country: US

NetRange: 199.104.128.0 - 199.104.137.255
CIDR: 199.104.128.0/21, 199.104.136.0/23
NetName: MOTOROLASPS
NetHandle: NET-199-104-128-0-2
Parent: NET-199-104-128-0-1
NetType: Reassigned
Comment: 
RegDate: 1994-10-20
Updated: 1994-08-23
199.104.137.69 - Domain Dossier - owner and registrar information, whois and DNS reco...  Page 3 of 3

RTechHandle:
RTechName:
RTechPhone:
RTechEmail:

OrgTechHandle:
OrgTechName:
OrgTechPhone:
OrgTechEmail:

# ARIN WHOIS database, last updated 2009-10-03 20:00

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>i2arl.motlabs.com</td>
<td>IN</td>
<td>A</td>
<td>199.104.137.69</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>motlabs.com</td>
<td>IN</td>
<td>SOA</td>
<td>server: dns1.motlabs.com</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email: root.dns1.motlabs.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 93</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 10800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 3600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 604800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 86400</td>
<td></td>
</tr>
<tr>
<td>motlabs.com</td>
<td>IN</td>
<td>NS</td>
<td>dns1.motlabs.com</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>motlabs.com</td>
<td>IN</td>
<td>NS</td>
<td>dns2.motlabs.com</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>motlabs.com</td>
<td>IN</td>
<td>HINFO</td>
<td>CPU: Motorola Labs</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OS: NONE</td>
<td></td>
</tr>
<tr>
<td>69.137.104.199.in-</td>
<td>IN</td>
<td>PTR</td>
<td>i2arl.motlabs.com</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>addr.arpa</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier  Investigate domains and IP addresses

<table>
<thead>
<tr>
<th>domain or IP address</th>
<th>204.14.95.58</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ domain whois record</td>
<td>✔ DNS records</td>
</tr>
<tr>
<td>✔ network whois record</td>
<td>❌ service scan</td>
</tr>
</tbody>
</table>

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

lookup failed 204.14.95.58

Could not find a domain name corresponding to this IP address.

Domain Whois record

Don't have a domain name for which to get a record

Network Whois record

Queried whois.arin.net with "204.14.95.58"...

OrgName: Fluid Hosting LLC
OrgID: FHL-12
Address: PO Box 453
City: Storrs
StateProv: CT
PostalCode: 06268-0453
Country: US

NetRange: 204.14.88.0 - 204.14.95.255
CIDR: 204.14.88.0/21
NetName: FHL-IPV4-01
NetHandle: NET-204-14-88-0-1
Parent: NET-204-0-0-0-0
NetType: Direct Allocation
NameServer: NS1.FLUIDHOSTING.NET
NameServer: NS2.FLUIDHOSTING.NET
Comment: 
RegDate: 2005-06-06
Updated: 2005-06-13

OrgTechHandle: NAD30-ARIN
OrgTechName: admin, network
OrgTechPhone: +1-877-584-0308
OrgTechEmail: admin@fluidhosting.com
DNS records

DNS query for 58.95.14.204.in-addr.arpa returned an error from the server: NameError

No records to display
Domain Dossier

Investigate domains and IP addresses

Domain or IP address: 206.123.88.43

- Domain WHOIS record
- DNS records
- Network WHOIS record
- Traceroute
- Service scan

Log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

Canonical name: lordvader.no-ip.biz.

Aliases: none

Addresses: 206.123.88.43

Domain WHOIS record

Queried whois.biz with "no-ip.biz"

Domain Name: NO-IP.BIZ
Domain ID: D1921163-BIZ
Sponsoring Registrar: VITALWERKS INTERNET SOLUTIONS, LLC
Sponsoring Registrar IANA ID: 1327
Domain Status: clientTransferProhibited
Registrant ID: NOIP49B70BC1B066
Registrant Name: Domain Operations No-IP.com
Registrant Organization: Vitalwerks Internet Solutions, LLC
Registrant Address1: 9585 Prototype Ct
Registrant Address2: Suite A
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89521
Registrant Country: United States
Registrant Country Code: US
Registrant Phone Number: +1.7758531883
Registrant Email: domains@no-ip.com
Administrative Contact ID: NOIP49B70BC1B066
Administrative Contact Name: Domain Operations No-IP.com
Administrative Contact Organization: Vitalwerks Internet Solutions, LLC
Administrative Contact Address1: 9585 Prototype Ct
Administrative Contact Address2: Suite A
Administrative Contact City: Reno
Administrative Contact State/Province: NV
Administrative Contact Postal Code: 89521
Administrative Contact Country: United States
Administrative Contact Country Code: US
Administrative Contact Phone Number: +1.7758531883
Administrative Contact Email: domains@no-ip.com

http://centralops.net/co/DomainDossier.aspx

10/3/2009
Billing Contact ID: NOIP49B70BC1B066
Billing Contact Name: Domain Operations No-IP.com
Billing Contact Organization: Vitalwerks Internet Solutions, LLC
Billing Contact Address1: 9585 Prototype Ct
Billing Contact Address2: Suite A
Billing Contact City: Reno
Billing Contact State/Province: NV
Billing Contact Postal Code: 89521
Billing Contact Country: United States
Billing Contact Country Code: US
Billing Contact Phone Number: +1.7758531883
Billing Contact Email: domains@no-ip.com
Technical Contact ID: NOIP49B70BC1B066
Technical Contact Name: Domain Operations No-IP.com
Technical Contact Organization: Vitalwerks Internet Solutions, LLC
Technical Contact Address1: 9585 Prototype Ct
Technical Contact Address2: Suite A
Technical Contact City: Reno
Technical Contact State/Province: NV
Technical Contact Postal Code: 89521
Technical Contact Country: United States
Technical Contact Country Code: US
Technical Contact Phone Number: +1.7758531883
Technical Contact Email: domains@no-ip.com
Name Server: NF1.NO-IP.COM
Name Server: NF2.NO-IP.COM
Name Server: NF3.NO-IP.COM
Name Server: NF4.NO-IP.COM
Created by Registrar: DIRECTNIC, LTD.
Last Updated by Registrar: VITALWERKS INTERNET SOLUTIONS, LLC
Last Transferred Date: Tue Aug 26 02:24:24 GMT 2008
Domain Registration Date: Thu Nov 22 23:09:20 GMT 2001
Domain Expiration Date: Wed Nov 21 23:59:59 GMT 2012
Domain Last Updated Date: Tue Aug 25 17:09:18 GMT 2009

>>> Whois database was last updated on: Sat Oct 03 20:45:21 GMT 2009 <<<

**Network Whois record**

Queried whois.arin.net with "!NET-206-123-88-0-1"

OrgName: Networld Internet Services
OrgID: NIS-116
Address: 100 Fairfield Dr.
City: Barto
StateProv: PA
PostalCode: 19504
Country: US

NetRange: 206.123.88.0 - 206.123.89.255
CIDR: 206.123.88.0/23
NetName: COLO4-NIS-116-013108
NetHandle: NET-206-123-88-0-1
Parent: NET-206-123-64-0-1
NetType: Reallocated
NameServer: NS3.TEKTONIC.NET
NameServer: NS4.TEKTONIC.NET
Comment:
RegDate: 2008-01-31
Updated: 2008-01-31

http://centralops.net/co/DomainDossier.aspx
OrgTechHandle: TECHN537-ARIN
OrgTechName: Technical Support
OrgTechPhone: +1-484-948-1124
OrgTechEmail: matta@tektonic.net

# ARIN WHOIS database, last updated 2009-10-03 20:00

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>lordvader.no-ip.biz</td>
<td>IN</td>
<td>A</td>
<td>206.123.88.43</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>SOA</td>
<td>server: nf1.no-ip.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email: hostmaster.no-ip.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 2029221398</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 300</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 604800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 600</td>
<td></td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>NS</td>
<td>nf2.no-ip.com</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>NS</td>
<td>nf4.no-ip.com</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>NS</td>
<td>nf1.no-ip.com</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>NS</td>
<td>nf3.no-ip.com</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>A</td>
<td>204.16.252.112</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail2.no-ip.com</td>
<td></td>
</tr>
<tr>
<td>no-ip.biz</td>
<td>IN</td>
<td>MX</td>
<td>preference: 5</td>
<td>60s (00:01:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail1.no-ip.com</td>
<td></td>
</tr>
<tr>
<td>43.88.123.206.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>lordvader.no-ip.biz</td>
<td>599s (00:09:59)</td>
</tr>
</tbody>
</table>

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier  Investigate domains and IP addresses

domain or IP address 206.123.89.201

☑ domain whois record  ☑ DNS records  ☐ traceroute
☑ network whois record  ☐ service scan  (go)

user: 65.214.169.254 [anonymous] 36/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name bocacentral.com.

aliases

addresses 206.123.89.201

Domain Whois record

Queried whois.internic.net with "dom bocacentral.com"

Domain Name: BOCACENTRAL.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS1.MYDYNDNS.ORG
Name Server: NS2.MYDYNDNS.ORG
Status: clientTransferProhibited
Updated Date: 01-sep-2008
Creation Date: 31-may-2004
Expiration Date: 31-may-2010

>>> Last update of whois database: Sun, 04 Oct 2009 04:37:29 UTC <<<

Queried whois.networksolutions.com with "bocacentral.com"

Registrant:

ATTN: BOCACENTRAL.COM
C/O Network Solutions
P.O. Box 447
Herndon, VA. 20172-0447

Domain Name: BOCACENTRAL.COM

Promote your business to millions of viewers for only $1 a month
Learn how you can get an Enhanced Business Listing here for your domain name.

Learn more at http://www.NetworkSolutions.com/

Administrative Contact: aq47d66973c@networksolutionsprivateregistration.com
ATTN: BOCACENTRAL.COM
C/o Network Solutions
P.O. Box 447
Herndon, VA 20172-0447

Technical Contact: Network Solutions, LLC.
customerservice@networksolutions.com
13861 Sunrise Valley Drive
Herndon, VA 20171
US
1-888-642-9675 fax: 571-434-4620

Record expires on 31-May-2010.
Record created on 31-May-2004.
Database last updated on 4-Oct-2009 00:35:06 EDT.

Domain servers in listed order:
NS1.MYDYNDNS.ORG
NS2.MYDYNDNS.ORG

This listing is a Network Solutions Private Registration. Mail correspondence to this address must be sent via USPS Express Mail(TM) or USPS Certified Mail(R); all other mail will not be processed. Be sure to include the registrant's domain name in the address.

Network Whois record

Queried whois.arin.net with "!NET-206-123-88-0-1"...

OrgName: Networld Internet Services
OrgID: NIS-116
Address: 100 Fairfield Dr.
City: Barto
StateProv: PA
PostalCode: 19504
Country: US
NetRange: 206.123.88.0 - 206.123.89.255
CIDR: 206.123.88.0/23
NetName: COLO4-NIS-116-013108
NetHandle: NET-206-123-88-0-1
Parent: NET-206-123-64-0-1
NetType: Reallocated
NameServer: NS3.TEKTONIC.NET
NameServer: NS4.TEKTONIC.NET
Comment:
RegDate: 2008-01-31
Updated: 2008-01-31
OrgTechHandle: TECHN537-ARIN
OrgTechName: Technical Support
OrgTechPhone: +1-484-948-1124
OrgTechEmail: 

http://centralops.net/co/DomainDossier.aspx
# ARIN WHOIS database, last updated 2009-10-03 20:00

## DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>201.89.123.206.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>bocacentral.com</td>
<td>600s (00:10:00)</td>
</tr>
</tbody>
</table>

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier

Investigate domains and IP addresses

- domain or IP address: 206.123.89.61
- domain whois record
- DNS records
- network whois record
- service scan

user: 65.214.169.254 [anonymous] 35/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name: vps.fddl.ca.

aliases
addresses: 206.123.89.61

Domain Whois record

Queried whois.cira.ca with "fddl.ca"...

Domain name: fddl.ca
Domain status: EXIST
Approval date: 2004/03/24
Renewal date: 2011/03/24
Updated date: 2009/02/19

Registrar:
Name: Tucows.com Co.
Number: 156

Name servers:
ns1.mdnsservice.com
ns2.mdnsservice.com
ns3.mdnsservice.com

Network Whois record

Queried whois.arin.net with "!NET-206-123-88-0-1"...

OrgName: Networld Internet Services
OrgID: NIS-116
Address: 100 Fairfield Dr.
City: Barto
StateProv: PA
PostalCode: 19504
Country: US

NetRange: 206.123.88.0 - 206.123.89.255

http://centralops.net/co/DomainDossier.aspx

10/3/2009
CIDR: 206.123.88.0/23
NetName: COLO4-NIS-116-013108
NetHandle: NET-206-123-88-0-1
Parent: NET-206-123-64-0-1
NetType: Reallocated
NameServer: NS3.TEKTONIC.NET
NameServer: NS4.TEKTONIC.NET
Comment:
RegDate: 2008-01-31
Updated: 2008-01-31

OrgTechHandle: TECHN537-ARIN
OrgTechName: Technical Support
OrgTechPhone: +1-484-948-1124
OrgTechEmail: matta@tektonic.net

# ARIN WHOIS database, last updated 2009-10-03 20:00

DNS records

DNS query for vps.fddl.ca returned an error from the server: NameError

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>fddl.ca</td>
<td>IN</td>
<td>SOA</td>
<td>server: ns1.mdnsservice.com</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email: hostmaster.mdnsservice.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 1038077600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 10001</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 7200</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 2419200</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 86400</td>
<td></td>
</tr>
<tr>
<td>fddl.ca</td>
<td>IN</td>
<td>NS</td>
<td>ns1.mdnsservice.com</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>fddl.ca</td>
<td>IN</td>
<td>NS</td>
<td>ns2.mdnsservice.com</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>fddl.ca</td>
<td>IN</td>
<td>NS</td>
<td>ns3.mdnsservice.com</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>fddl.ca</td>
<td>IN</td>
<td>MX</td>
<td>preference: 0</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: smtp.secureserver.net</td>
<td></td>
</tr>
<tr>
<td>fddl.ca</td>
<td>IN</td>
<td>A</td>
<td>64.6.250.4</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td>fddl.ca</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>300s (00:05:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mailstore1.secureserver.net</td>
<td></td>
</tr>
<tr>
<td>61.89.123.206.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>vps.fddl.ca</td>
<td>599s (00:09:59)</td>
</tr>
</tbody>
</table>

-- end --
URL for this output | return to CentralOps.net, a service of Hexillion

http://centralops.net/co/DomainDossier.aspx

10/3/2009
Domain Dossier
Investigate domains and IP addresses

domain or IP address: 209.216.0.196

- domain whois record
- DNS records
- traceroute

network whois record
- service scan

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name: 209.216.0.196.static.sna.hosting.com.

aliases
addresses: 209.216.0.196

Domain Whois record
Queried whois.internic.net with "dom hosting.com"...

Domain Name: HOSTING.COM
Registrar: TUCOWS INC.
Whois Server: whois.tucows.com
Referral URL: http://domainhelp.opensrs.net
Name Server: AUTH01.NS.HOSTING.COM
Name Server: AUTH02.NS.HOSTING.COM
Name Server: AUTH03.NS.HOSTING.COM
Name Server: AUTH04.NS.HOSTING.COM
Name Server: AUTH05.NS.HOSTING.COM
Name Server: AUTH06.NS.HOSTING.COM
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 18-dec-2008
Creation Date: 08-feb-1996
Expiration Date: 09-feb-2015

>>> Last update of whois database: Sun, 04 Oct 2009 04:38:46 UTC <<<

Queried whois.tucows.com with "hosting.com"...

Registrant:
HOSTING.COM
Express Technologies
PO Box 22789
Louisville, KY 40252
US

Domain name: HOSTING.COM

Administrative Contact:
Hostmaster, Domain domainsupport@wsmdomains.com
Express Technologies
PO Box 22789
Louisville, KY 40252
US
+01.5022144100

Technical Contact:
Hostmaster, Domain domainsupport@wsmdomains.com
Express Technologies
PO Box 22789
Louisville, KY 40252
US
+01.5022144100

Registration Service Provider:
WSM Domains retail - 24/7 Support -502-214-4123, domainsupport@wsmdomains.com
1-800-455-1795
502-214-4140 (fax)
https://www.wsmdomains.com/help/support.html
Register your domain today! www.wsmdomains.com
Full DNS management - Free URL forwarding
Host with the family of Hosting.com companies

Registrar of Record: TUCOWS, INC.
Record last updated on 18-Dec-2008.
Record expires on 09-Feb-2015.
Record created on 08-Feb-1996.

Registrar Domain Name Help Center:
http://domainhelp.tucows.com

Domain servers in listed order:
AUTH06.NS.HOSTING.COM 209.164.46.41
AUTH02.NS.HOSTING.COM 130.94.6.154
AUTH04.NS.HOSTING.COM 130.94.6.155
AUTH01.NS.HOSTING.COM 199.231.136.10
AUTH03.NS.HOSTING.COM 65.182.208.250
AUTH05.NS.HOSTING.COM 209.164.46.40

Domain status: clientTransferProhibited
clientUpdateProhibited

Network Whois record

Queried whois.arin.net with "209.216.0.196"

OrgName: WCP/32POINTS INTERMEDIATE HOLDING COMPANY, INC.
OrgID: WCP32
Address: 1400 Glenarm Place
Address: Suite 100
City: Denver
StateProv: CO
PostalCode: 80202
Country: US

NetRange: 209.216.0.0 - 209.216.63.255
CIDR: 209.216.0.0/18
NetName: IRVINE-209-216-0-0-18
NetHandle: NET-209-216-0-0-1
Parent: NET-209-0-0-0-0
NetType: Direct Allocation
NameServer: AUTH01.NS.HOSTING.COM
NameServer: AUTH02.NS.HOSTING.COM
NameServer: AUTH03.NS.HOSTING.COM
NameServer: AUTH04.NS.HOSTING.COM
NameServer: AUTH05.NS.HOSTING.COM
Comment:
RegDate: 1998-03-20
Updated: 2009-07-17

OrgAbuseHandle: ABUSE1072-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-302-731-4948
OrgAbuseEmail: abuse@hostmysite.com

OrgTechHandle: IPADM271-ARIN
OrgTechName: IP Admin
OrgTechPhone: +1-302-731-4948
OrgTechEmail: ipadmin@hostmysite.com

# ARIN WHOIS database, last updated 2009-10-03 20:00

DNS records
DNS query for *hosting.com* failed: **MessageTruncated**

DNS query for *hosting.com* failed: **MessageTruncated**

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time t</th>
</tr>
</thead>
<tbody>
<tr>
<td>209.216.0.196.static.sna.hosting.com</td>
<td>IN</td>
<td>A</td>
<td>209.216.0.196</td>
<td>43200</td>
</tr>
<tr>
<td>hosting.com</td>
<td>IN</td>
<td>A</td>
<td>209.41.173.123</td>
<td>301</td>
</tr>
<tr>
<td>hosting.com</td>
<td>IN</td>
<td>NS</td>
<td>auth01.ns.hosting.com</td>
<td>301</td>
</tr>
<tr>
<td>hosting.com</td>
<td>IN</td>
<td>NS</td>
<td>auth03.ns.hosting.com</td>
<td>301</td>
</tr>
<tr>
<td>hosting.com</td>
<td>IN</td>
<td>NS</td>
<td>auth06.ns.hosting.com</td>
<td>301</td>
</tr>
<tr>
<td>hosting.com</td>
<td>IN</td>
<td>NS</td>
<td>auth02.ns.hosting.com</td>
<td>301</td>
</tr>
<tr>
<td>hosting.com</td>
<td>IN</td>
<td>NS</td>
<td>auth04.ns.hosting.com</td>
<td>301</td>
</tr>
</tbody>
</table>
hosting.com  IN  NS  auth05.ns.hosting.com  301
hosting.com  IN  MX  preference:  300  exchange:  hosting.com.s5b1.psmtp.com  301
hosting.com  IN  MX  preference:  400  exchange:  hosting.com.s5b2.psmtp.com  301
hosting.com  IN  MX  preference:  100  exchange:  hosting.com.s5a1.psmtp.com  301
hosting.com  IN  MX  preference:  200  exchange:  hosting.com.s5a2.psmtp.com  301

196.0.216.0.196.in-addr.arpa  IN  PTR  209.216.0.196.static.sna.hosting.com  4320C

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
**Domain Dossier**  Investigate domains and IP addresses

<table>
<thead>
<tr>
<th>domain or IP address</th>
<th>212.27.191.167</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ domain whois record</td>
<td></td>
</tr>
<tr>
<td>✓ DNS records</td>
<td></td>
</tr>
<tr>
<td>✓ network whois record</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

user: 65.214.169.254 [anonymous] 33/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

**Address lookup**

lookup failed 212.27.191.167

*Could not find a domain name corresponding to this IP address.*

**Domain Whois record**

Don't have a domain name for which to get a record

**Network Whois record**

Queried **whois.ripe.net** with "-B 212.27.191.167"

% Information related to '212.27.191.128 - 212.27.191.255'

| inetnum:    | 212.27.191.128 - 212.27.191.255 |
| netname:    | UNITAR-CH                        |
| descr:      | UNITAR                           |
| desc:       | GENEVA                           |
| country:    | CH                               |
| admin-c:    | RV1873-RIPE                      |
| tech-c:     | RV1873-RIPE                      |
| status:     | ASSIGNED PA                      |
| notify:     | ripe-notify@psineteurope.com     |
| mnt-by:     | PSINETBU-VIA-MNT                 |
| changed:    | network-ripe@psineteurope.co.uk  |
| changed:    | 20041125                         |
| source:     | RIPE                             |

person:          
address:         
address:         
address:         
phone:           
fax-no:          
e-mail:          
nic-hdl:         
notify:          

http://centralops.net/co/DomainDossier.aspx
notify: ripe-notify@uk.psi.com
mnt-by: PSINET-UK-SYSADMIN
changed: 
source: RIPE

% Information related to '212.27.160.0/19AS8928'

route: 212.27.160.0/19
descr: CH-PSINET-990412
origin: AS8928
mnt-by: PSINETBE-VIA-MNT
changed: network-ripe@psineteurope.co.uk 20040803
changed: langa10@interoute.net 20070523
source: RIPE

DNS records

DNS query for 167.191.27.212.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier  Investigate domains and IP addresses

domain or IP address 212.37.47.24

☑ domain whois record ☑ DNS records ☑ traceroute
☑ network whois record ☑ service scan  

user: 65.214.169.254 [anonymous] 32/50
log in | get account

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name 24.booms-edv.de.

aliases
addresses 212.37.47.24

Domain Whois record

Queried whois.denic.de with ":T new,ace,dn -C UTF-8 booms-edv.de"

Domain: booms-edv.de
Domain-Ace: booms-edv.de
Nserver: dns1.booms-edv.de 212.37.47.21
Nserver: bl.rsns.hosteurope.de
Status: connect
Changed: 2009-07-16T19:19:22+02:00

[Tech-C]
Type: PERSON
Name: info@booms-edv.de
Address: http://centralops.net/ co/DomainDossier.aspx
Phone: 10/3/2009

Fax: +492381671215
Email: info@booms-edv.de
Changed: 2004-10-11T16:54:08+02:00

Network Whois record

Queried whois.ripe.net with "-B 212.37.47.24"

% Information related to '212.37.47.16 - 212.37.47.31'

inetnum: 212.37.47.16 - 212.37.47.31
netname: BOOMS-EDV
descr: Booms EDV
descr: Herrenstrasse 10
descr: D-59073 Hamm
descr: Germany
country: DE
admin-c: TB1722-RIPE
tech-c: HAMM2-RIPE
status: ASSIGNED PA
remarks: Send hack and spam complaints to
mnt-by: AS12355-MNT
mnt-lower: AS12355-MNT
mnt-routes: AS12355-MNT
changed: hostmaster@helinet.de 20040322
source: RIPE

role: Hamcom Hostmaster
address: HeLi NET Telekommunikation GmbH & Co. KG
address: Hafenstrasse 80-82
address: D-59067 Hamm
address: Germany
phone: +49 2381 874 4250
fax-no: +49 2381 874 1007
e-mail: hostmaster@helinet.de
e-mail: postmaster@helinet.de
admin-c: OZII-RIPE
admin-c: MKL19-RIPE
admin-c: PK3224-RIPE
tech-c: MKL19-RIPE
tech-c: PK3224-RIPE
nic-hdl: HAMM2-RIPE
remarks: Send hack-, spam- and abuse complaints
remarks: to abuse-mailbox only!
remarks: ALL OTHERS WILL BE TRASHED!
abuse-mailbox: abuse@helinet.de
notify: hostmaster@helinet.de
mnt-by: AS12355-MNT
changed: hostmaster@hamcom.de 20010410
changed: hostmaster@hamcom.de 20010417
changed: hostmaster@hamcom.de 20020305
changed: hostmaster@hamcom.de 20020320
changed: hostmaster@hamcom.de 20020404
changed: hostmaster@hamcom.de 20021016
changed: hostmaster@helinet.de 20040326
changed: mk@helinet.de 20051109
changed: pk@helinet.de 20060713
changed: mk@helinet.de 20070330
changed: mk@helinet.de 20090602
source: RIPE
DNS records

DNS query for **24.booms-edv.de** returned an error from the server: **NameError**

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>booms-edv.de</td>
<td>IN</td>
<td>SOA</td>
<td>server: dns1.booms-edv.de</td>
<td>172800s (2.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email: root.booms-edv.de</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 2009071601</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 28800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 3600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 864000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 43200</td>
<td></td>
</tr>
<tr>
<td>booms-edv.de</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>172800s (2.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail.booms-edv.de</td>
<td></td>
</tr>
<tr>
<td>booms-edv.de</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>172800s (2.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: vmail.booms-edv.de</td>
<td></td>
</tr>
<tr>
<td>booms-edv.de</td>
<td>IN</td>
<td>NS</td>
<td>b1.rsns.hosteurope.de</td>
<td>172800s (2.00:00:00)</td>
</tr>
<tr>
<td>booms-edv.de</td>
<td>IN</td>
<td>NS</td>
<td>dns1.booms-edv.de</td>
<td>172800s (2.00:00:00)</td>
</tr>
<tr>
<td>booms-edv.de</td>
<td>IN</td>
<td>A</td>
<td>212.37.47.24</td>
<td>172800s (2.00:00:00)</td>
</tr>
</tbody>
</table>
24.47.37.212.in-addr.arpa IN PTR 24.booms-edv.de 86400s (1.00:00:00)

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier  Investigate domains and IP addresses

domain or IP address  212.5.37.160

✔ domain whois record  ✔ DNS records  □ traceroute

✔ network whois record  □ service scan  99

user: 65.214.169.254 [anonymous]  31/50
log in | get account

centralOps.net

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

canonical name  ip-212.5.37.160.netcomlan.com.
aliases
addresses  212.5.37.160

Domain Whois record

Queried whois.internic.net with "dom netcomlan.com"...

Domain Name: NETCOMLAN.COM
Registrar: DIRECTI INTERNET SOLUTIONS PVT. LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Whois Server: whois.PublicDomainRegistry.com
Referral URL: http://www.PublicDomainRegistry.com
Name Server: REDIRNS1.BGDNS.NET
Name Server: REDIRNS2.BGDNS.NET
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 08-apr-2009
Creation Date: 15-mar-2005
Expiration Date: 15-mar-2011

>>> Last update of whois database: Sun, 04 Oct 2009 05:36:51 UTC <<<

Queried whois.publicdomainregistry.com with "netcomlan.com"...

The data in this whois database is provided to you for information purposes only, that is, to assist you in obtaining information about or related to a domain name registration record. We make this information available "as is", and do not guarantee its accuracy. By submitting a whois query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) enable high volume, automated, electronic processes that stress or load this whois database system providing you this information; or (2) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone. The compilation, repackaging, dissemination or other use of this data is expressly prohibited without prior written consent from us. The Registrar of record is Directi Internet Solutions Pvt.
We reserve the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.

This domain is registered by: Host.bg

Domain Name: NETCOMLAN.COM

Registrant:

Tel.
Fax.

Creation Date: 15-Mar-2005
Expiration Date: 15-Mar-2011

Domain servers in listed order:
redirnsl.bgdns.net
redirns2.bgdns.net

Administrative Contact:

NetCom Networks

Tel.

Technical Contact:

NedKom-7 OOD

Tel.

Status: LOCKED
Note: This Domain Name is currently Locked. In this status the domain name cannot be transferred, hijacked, or modified. The Owner of this domain name can easily change this status from their control panel. This feature is provided as a security measure against fraudulent domain name.

Host.bg - leading Bulgarian hosting provider.

Network Whois record

Queried whois.ripe.net with "-B 212.5.37.160"...

http://centralops.net/co/DomainDossier.aspx
% Information related to '212.5.32.0 - 212.5.44.255'

inetnum: 212.5.32.0 - 212.5.44.255
netname: NETCOM-SAMOKOV
descr: Netcom Ltd
country: BG
admin-c: KT1269-RIPE
tech-c: KT1269-RIPE
status: ASSIGNED PA
mnt-by: IPACCT-MNT
changed: 
source: RIPE

% Information related to '212.5.32.0/20AS47849'

route: 212.5.32.0/20
descr: Netcom Ltd.
origin: AS47849
mnt-by: IPACCT-MNT
changed: 
source: RIPE

dns records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-212.5.37.160.netcomlan.com</td>
<td>IN</td>
<td>A</td>
<td>212.5.36.4</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>ip-212.5.37.160.netcomlan.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail.netcomlan.com</td>
<td></td>
</tr>
<tr>
<td>netcomlan.com</td>
<td>IN</td>
<td>SOA</td>
<td>server: redirns1.bgdns.net</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>email:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>serial: 2005020407</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>refresh: 3600</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>retry: 1800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expire: 86400</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>minimum ttl: 300</td>
<td></td>
</tr>
<tr>
<td>netcomlan.com</td>
<td>IN</td>
<td>NS</td>
<td>redirns2.bgdns.net</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>netcomlan.com</td>
<td>IN</td>
<td>NS</td>
<td>redirns1.bgdns.net</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>netcomlan.com</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exchange: mail.netcomlan.com</td>
<td></td>
</tr>
</tbody>
</table>
netcomlan.com  IN  A    212.5.36.4     86400s (1:00:00:00)
160.37.5.212.in-addr.arpa  IN  PTR  ip-212.5.37.160.netcomlan.com  14400s (04:00:00)

-- end --
URL for this output | return to CentralOps.net, a service of Hexillion
Domain Dossier

Investigate domains and IP addresses

Domain or IP address: 213.146.173.66

- Domain whois record
- DNS records
- Network whois record
- Service scan


New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

Canonical name: udala.tribalforge.net.

Aliases

Addresses: 213.146.173.66

Domain Whois record

Queried whois.internic.net with "dom tribalforge.net"...

Domain Name: TRIBALFORGE.NET
Registrar: TUCOWS INC.
Whois Server: whois.tucows.com
Referral URL: http://domainhelp.opensrs.net
Name Server: NS18.ZONEEDIT.COM
Name Server: NS8.ZONEEDIT.COM
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 14-apr-2009
Creation Date: 05-may-2005
Expiration Date: 05-may-2011

>>> Last update of whois database: Sun, 04 Oct 2009 05:38:08 UTC <<<

Queried whois.tucows.com with "tribalforge.net"...

Registrant:
Tribal Ltd.
Davidson House
Forbury Square
Reading, Berkshire RG1 3EU
GB

Domain name: TRIBALFORGE.NET

Administrative Contact:

Davidson House
Forbury Square
Reading, Berkshire RG1 3EU
GB
+44.1189001370

Technical Contact:
Ltd, GX Networks services@123-reg.co.uk
5 Roundwood Avenue
Stockley Park
Uxbridge, Middlesex UB11 1FF
GB
+44.48712309525 Fax: +44.8701650437

Registration Service Provider:
services@123-reg.co.uk
08712309525
08709126612 (fax)
http://www.123-reg.co.uk
This company may be contacted for domain login/passwords,
DNS/Nameserver changes, and general domain support questions.

Registrar of Record: TUCOWS, INC.
Record last updated on 14-Apr-2009.
Record expires on 05-May-2011.
Record created on 05-May-2005.

Registrar Domain Name Help Center:
http://domainhelp.tucows.com

Domain servers in listed order:
NS18.ZONEEDIT.COM
NS8.ZONEEDIT.COM

Domain status: clientTransferProhibited
clientUpdateProhibited

Network Whois record
Queried whois.ripe.net with "-B 213.146.173.66"

% Information related to '213.146.173.64 - 213.146.173.95'

inetnum: 213.146.173.64 - 213.146.173.95
netname: PA-TRIBAL
descr: Tribal Internet Limited
country: GB
admin-c: TB3847-RIPE
tech-c: TB3847-RIPE
tech-c: CGNT-RIPE
status: ASSIGNED PA
mnt-by: COGENT-HM-MNT
changed: COGENT-HM-MNT
source: RIPE
role: Cogent Communications Hostmaster
address: Cogent Communications, Inc.

1015 31st Steet NW
Washington, DC 20007
USA

phone: +1 703 657 7904

abuse-mailbox: abuse@cogentco.com
admin-c: JK4128-RIPE
tech-c: CCRRA-RIPE
tech-c: WG777-RIPE
tech-c: GR2753-RIPE
tech-c: MC1557-RIPE
tech-c: JK4128-RIPE
nic-hdl: CGNT-RIPE
mnt-by: COGENT-ROOT-MNT
changed:

person: Tribal Internet Limited
address: Davidson House, Forbury Square
RG1 3EU Reading
GB

phone:
e-mail:
nic-hdl: TB3847-RIPE
mnt-by: COGENT-HM-MNT
changed:

source: RIPE

% Information related to '213.146.160.0/19AS174'

route: 213.146.160.0/19
descr: Cogent Communications, Inc.
origin: AS174
mnt-by: COGENT-ROUTE-MNT
changed:

source: RIPE

DNS records

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>udala.tribalforge.net</td>
<td>IN</td>
<td>A</td>
<td>213.146.173.66</td>
<td>7200s (02:00:00)</td>
</tr>
<tr>
<td>tribalforge.net</td>
<td>IN</td>
<td>A</td>
<td>213.131.169.116</td>
<td>7200s (02:00:00)</td>
</tr>
<tr>
<td>tribalforge.net</td>
<td>IN</td>
<td>NS</td>
<td>ns18.zoneedit.com</td>
<td>7200s (02:00:00)</td>
</tr>
<tr>
<td>tribalforge.net</td>
<td>IN</td>
<td>NS</td>
<td>ns8.zoneedit.com</td>
<td>7200s (02:00:00)</td>
</tr>
</tbody>
</table>

http://centralops.net/co/DomainDossier.aspx

10/3/2009
tribalforge.net  IN  SOA  server: ns18.zoneedit.com  7200s (02:00:00)
email: soacontact.zoneedit.com
serial: 1226093566
refresh: 14400
retry: 7200
expire: 950400
minimum 7200
ttl: 

66.173.146.213.in-addr.arpa  IN  PTR  udala.tribalforge.net  10798s (02:59:58)

-- end --
Domain Dossier  Investigate domains and IP addresses

domain or IP address 213.163.176.210
✓ domain whois record ✓ DNS records  
✓ network whois record ✓ traceroute

user: 65.214.169.254 [anonymous] 28/50
log in | get account

centralops.net

New: Compare web hosting plans across multiple providers: shared | VPS | dedicated

Address lookup

lookup failed 213.163.176.210

Could not find a domain name corresponding to this IP address.

Domain Whois record

Don't have a domain name for which to get a record

Network Whois record

Queried whois.ripe.net with "-B 213.163.176.210"

% Information related to '213.163.160.0 - 213.163.191.255'

inetnum: 213.163.160.0 - 213.163.191.255
org: ORG-K01-RIPE
netname: PR-KHEOPS-20010514
descr: Kheops Organisation
descr: PROVIDER Local Registry
country: FR
admin-c: SC3533-RIPE
tech-c: SC3533-RIPE
status: ALLOCATED PA
notify: sc@kheops.org
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: MNT-KHEOPS-ORGANISATION
mnt-routes: MNT-KHEOPS-ORGANISATION
mnt-domains: MNT-KHEOPS-ORGANISATION
changed: hostmaster@ripe.net 20010514
changed: hostmaster@ripe.net 20010705
changed: hostmaster@ripe.net 20040525
source: RIPE

organisation: ORG-K01-RIPE
org-name: Kheops Organisation
org-type: LIR
descr: KHEOPS ORGANISATION Global Network Solutions
address: Kheops Organisation  
  Centre d'affaires La Boursidiere  
  BP 62  
  93357 Le Plessis Robinson Cedex  
  FRANCE  

phone: +33 141 360 010  
fax-no: +33 141 360 019  
e-mail:  
admin-c: AM16863-RIPE  
admin-c: SC3533-RIPE  
admin-c: MB16774-RIPE  
mnt-ref: RIPE-NCC-HM-MNT  
mnt-ref: MNT-KHEOPS-ORGANISATION  
notify:  
mnt-by: RIPE-NCC-HM-MNT  
changed: hostmaster@ripe.net 20040415  
changed: hostmaster@ripe.net 20040525  
changed: bitbucket@ripe.net 20060220  
changed: bitbucket@ripe.net 20060327  
changed: bitbucket@ripe.net 20060906  
changed: bitbucket@ripe.net 20060907  
changed: bitbucket@ripe.net 20070803  
changed: bitbucket@ripe.net 20070803  
changed: bitbucket@ripe.net 20070831  
changed: bitbucket@ripe.net 20080922  
changed: bitbucket@ripe.net 20080922  
source: RIPE

% Information related to '213.163.160.0/19AS20917'

route: 213.163.160.0/19  
descr:  
origin: AS20917  
notify:  
mnt-lower: MNT-KHEOPS-ORGANISATION  
mnt-routes: MNT-KHEOPS-ORGANISATION  
mnt-by: MNT-KHEOPS-ORGANISATION  
changed:  
source: RIPE

DNS records

DNS query for 210.176.163.213.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --
Total Deleted Page(s) = 75
Page 4 ~ b3; b6; b7C;
Page 5 ~ Referral/Direct;
Page 6 ~ Referral/Direct;
Page 7 ~ Referral/Direct;
Page 8 ~ b3; b6; b7C;
Page 9 ~ b3;
Page 10 ~ b3;
Page 11 ~ b3;
Page 12 ~ b3;
Page 13 ~ b3;
Page 14 ~ b3;
Page 15 ~ b3;
Page 16 ~ b3;
Page 17 ~ b7E;
Page 19 ~ b3; b6; b7C;
Page 20 ~ Referral/Direct;
Page 21 ~ Referral/Direct;
Page 22 ~ b3; b6; b7C;
Page 23 ~ b3; b6; b7C;
Page 24 ~ b3;
Page 25 ~ b3;
Page 26 ~ b3;
Page 27 ~ b3;
Page 28 ~ b3;
Page 29 ~ b3;
Page 30 ~ b3;
Page 31 ~ b3;
Page 32 ~ b3;
Page 33 ~ b3;
Page 34 ~ b3;
Page 35 ~ b3;
Page 36 ~ b3;
Page 37 ~ b3;
Page 38 ~ b3;
Page 39 ~ b3;
Page 40 ~ b3;
Page 41 ~ b3;
Page 42 ~ b3;
Page 43 ~ b3;
Page 44 ~ b3;
Page 45 ~ b3;
Page 46 ~ b3;
Page 47 ~ b3;
Page 48 ~ b3;
Page 49 ~ b3;
Page 50 ~ b3;
Page 51 ~ b3;
Page 52 ~ b3;
Serial # of Originating Document: 1
Date Received: 12/03/2009
From: 

By: 

To Be Returned: Yes
Receipt Given: No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure: Yes
Federal Taxpayer Information (FTI): No

Title: 

Reference: FD-802 re FGJ subpoena response from

Description: Original notes re interview of FGJ subpoena response from
FD-340 (Rev. 4-11-01)

File Number

Field Office Acquiring Evidence

Serial # of Originating Document

Date Received 10/14/2008

From

By

To Be Returned □ Yes □ No
Receipt Given □ Yes □ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
□ Yes □ No

Federal Taxpayer Information (FTI)
□ Yes □ No

Title:

Reference: FC-302 re review d

Description: □ Original notes re interview of

Subpoena response from
Potential Intel Value: Yes □ No □
Reviewed By: [Signature] Date: 2/23/2018
S-Drive Location: