U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

August 31, 2009

MS MARCIA HOFMANN
ELECTRONIC FRONTIER FOUNDATION
454 SHOTWELL STREET
SAN FRANCISCO, CA 94110

Subject: SKYPE (FBI SURVEILLANCE OF SKYPE COMMUNICATIONS)

FOIPA No. 1110910- 000

Dear Ms. Hofmann:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552		Section 552a
☒(b)(1)	☐(b)(7)(A)	☐(d)(5)
☒(b)(2)	☐(b)(7)(B)	☐(j)(2)
☐(b)(3)_____	☒(b)(7)(C)	☐(k)(1)
_____	☐(b)(7)(D)	☐(k)(2)
_____	☒(b)(7)(E)	☐(k)(3)
_____	☐(b)(7)(F)	☐(k)(4)
☒(b)(4)	☐(b)(8)	☐(k)(5)
☒(b)(5)	☐(b)(9)	☐(k)(6)
☒(b)(6)		☐(k)(7)

388 **page(s)** were reviewed and 221 **page(s)** are being released.

☐ Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:

- ☐ referred to the OGA for review and direct response to you.
- ☐ referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy, U.S. Department of Justice,1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident,

references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☐ See additional information which follows.

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 be 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 be reasonably 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 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

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 124
Page 15 ~ b2, b7E
Page 16 ~ b2, b7E
Page 34 ~ b2, b7E
Page 37 ~ b2, b7E
Page 38 ~ b2, b7E
Page 39 ~ b2, b7E
Page 40 ~ b2, b7E
Page 41 ~ b2, b7E
Page 42 ~ b2, b7E
Page 43 ~ b2, b7E
Page 44 ~ b2, b7E
Page 45 ~ b2, b7E
Page 46 ~ b2, b7E
Page 47 ~ b2, b7E
Page 48 ~ b2, b7E
Page 49 ~ b2, b7E
Page 50 ~ b2, b6, b7C, b7E
Page 54 ~ b2, b7E
Page 55 ~ b1, b2, b7E
Page 56 ~ b1, b2, b7E
Page 57 ~ b1, b2, b7E
Page 58 ~ b1, b2, b7E
Page 59 ~ b1, b2, b7E
Page 60 ~ b2, b7E
Page 85 ~ b2, b7E
Page 92 ~ b2, b7E
Page 95 ~ b2, b7E
Page 96 ~ b2, b7E
Page 97 ~ b2, b7E
Page 98 ~ b2, b7E
Page 99 ~ b2, b7E
Page 121 ~ b2, b7E
Page 123 ~ b2, b5, b7E
Page 124 ~ b2, b5, b7E
Page 125 ~ b2, b5, b7E
Page 126 ~ b2, b5, b7E
Page 127 ~ b2, b5, b7E
Page 128 ~ b2, b5, b7E
Page 129 ~ b2, b5, b7E
Page 131 ~ b2, b5, b7E
Page 132 ~ b2, b5, b7E
Page 133 ~ b2, b5, b7E
Page 134 ~ b2, b5, b7E
Page 139 ~ b2, b5, b7E

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 43
Page 7 ~ b2, b6, b7C, b7E
Page 8 ~ b1, b2, b6, b7C, b7E
Page 9 ~ b1, b2, b6, b7C, b7E
Page 10 ~ b1, b2, b6, b7C, b7E
Page 11 ~ b2, b6, b7C, b7E
Page 12 ~ b2, b6, b7C, b7E
Page 15 ~ b2, b7E
Page 16 ~ b2, b7E
Page 17 ~ b2, b7E
Page 18 ~ b2, b7E
Page 19 ~ b1, b2, b7E
Page 20 ~ b1, b2, b7E
Page 21 ~ b2, b7E
Page 22 ~ b1, b2, b7E
Page 25 ~ b2, b7E
Page 27 ~ b2, b7E
Page 32 ~ b2, b7E
Page 34 ~ b4
Page 37 ~ b1, b2, b7E
Page 38 ~ b1, b2, b7E
Page 40 ~
Copyrighted Material
Page 41 ~
Copyrighted Material

Page 42 ~
Copyrighted Material

Page 43 ~
Copyrighted Material

Page 44 ~
Copyrighted Material

Page 45 ~
Copyrighted Material

Page 46 ~
Copyrighted Material

Page 47 ~
Copyrighted Material

Page 48 ~

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

STATUS REPORT

Name	[redacted]
Week Ending	**20070209**

b6
b7C

ACCOMPLISHMENTS:

- Engineer meeting followup
- [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

ON-GOING WORK:

- [redacted]

b2
b7E

- Skype discussion writeup

FUTURE WORK:

- [redacted]

ISSUES:

-

TRAVEL:

-

LES

STATUS REPORT

b6
b7C

Name	
Week Ending	**20070223**

ACCOMPLISHMENTS:

-
-
-
-
- Working group topic development
- Inspection related logistics support
- Security training (annual requirement)

ON-GOING WORK:

-
-
-
-

b2
b7E

FUTURE WORK:

-
-
-

ISSUES:

- Monday holiday

TRAVEL:

LES

February 2007 RDD STATUS REPORT

[redacted]20070305

b6
b7C

[redacted]

- Skype discussion writeup
- [redacted]
- Status of helpdesk items ordered
- [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

Future Work

- [redacted]

b2
b7E

Travel

- [redacted]
- March 26-30 LV
- Tampa, Feb 5-6, 2007
- [redacted]

Meetings

STATUS REPORT

Name	[redacted]
Week Ending	**20070216**

b6
b7C

ACCOMPLISHMENTS:

- [redacted]
- Discuss TAWG Nellis AFB attendance
- Document hardware project capabilities for FBInet
- [redacted]
- [redacted]
- Completed FBI Security Awareness Training for 2007
- Completed PED forms
- Department manager meeting
- OTD SPTU-P2 meeting and discussion
- Second interviews [redacted]

b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

b2
b7E

ON-GOING WORK:

- [redacted]

FUTURE WORK:

- [redacted]

ISSUES:

-

TRAVEL:

-

LES

June 2008 RDD STAO/ROU STATUS REPORT

[redacted]20080602

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

ACCOMPLISHMENTS:

[redacted]

- Assisted [redacted] in obtaining equipment and troubleshooting new development server

[redacted]

- Assisted ROU by helping escort the movers

[redacted]

- Completed initial load & configuration of UC laptop

[redacted]

- Completed the Thology briefing at QTD, Quantico

[redacted]

- Created Roles and Goles for new hire [redacted]

b2
b6
b7C
b7E

[redacted]

- Documented Lead Operator roles and responsibilities

[redacted]

- Edit work breakdown for managers
- Escorted [redacted] to Quantico successfully obtaining his SACS badge
- Facilitated getting 11 File Cabinets re-keyed and escorted the locksmith during this initiative.

[redacted] The move is anticipated to close on today, 5/30/2008. [redacted] The move was completed with zero official incidents or violations

b6
b7C

February 2007 RDD STATUS REPORT

[redacted] 20070305

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

Accomplishments

[redacted]

- Assisted the unit in preparation for insnection matters

[redacted]

- Many meetings to plan for upcoming events - coordinate with OTD, and lots of time spent on audits and inspections

b2
b7E

[redacted]

- Cleared my required inventory inspection

[redacted]

- Completed FBI Security Awareness Training for 2007

b2
b6
b7C
b7E

[redacted]

- Discuss TAWG Nellis AFB attendance

[redacted]

b2
b7E

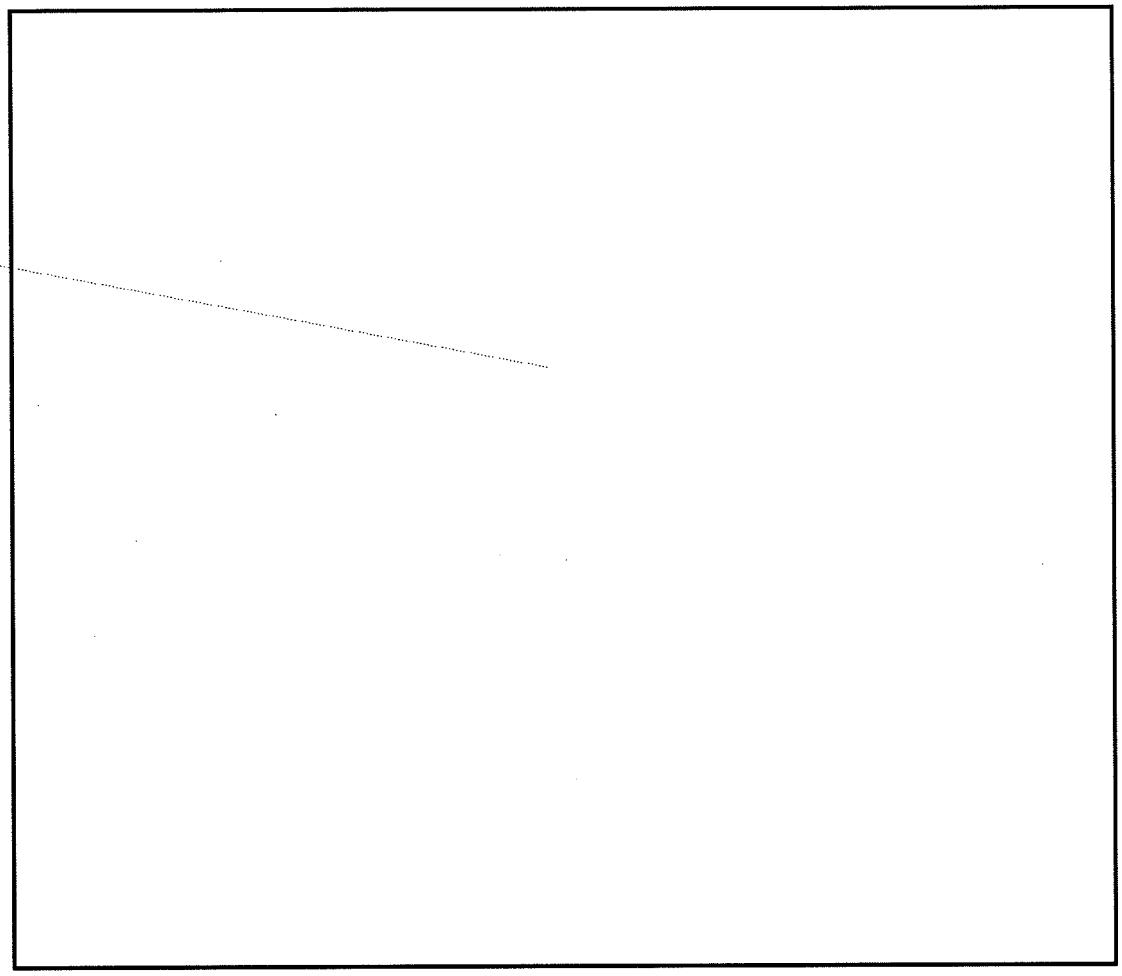
- Finalized presentation for Tampa trip

[redacted]

b2
b6
b7C
b7E

b1
b2
b7E

(S)



SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

From: [redacted] (OTD) (FBI)
Sent: Friday, June 29, 2007 3:12 PM
To: [redacted] (OTD) (FBI)
Subject: FW: Pre-Deployment Questions for Locating Computers

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SECRET

DATE: 11-24-2008
CLASSIFIED BY 60322/UCLRP/PJ/EHL
REASON: 1.4 (c)
DECLASSIFY ON: 11-24-2033

b1
b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

SENSITIVE BUT UNCLASSIFIED

From: [redacted] (OTD) (FBI)
Sent: Thursday, May 31, 2007 1:42 PM

b6
b7C

SECRET

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI) b6 b7C
Sent: Friday, June 29, 2007 3:09 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: [redacted] b2 b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

DATE: 11-24-2008
CLASSIFIED BY 60322/UCLRP/PJ/EHL
REASON: 1.4 (c)
DECLASSIFY ON: 11-24-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2 b7E

[redacted] Ideally once you have this filled out it could be copied and pasted into the KMS.

I defer to [redacted] to discuss the wording of the legal documents. b6 b7C

J...

[redacted] b2 b7E

Case Number

Warrant Expiration Date

Type of install - [redacted]

[redacted] b2 b7E

Info about the target computer:

[redacted]

[redacted] b2 b7E

(S) b1

[redacted]

Post Installation

Keep in mind that once we are installed we usually have the ability to:

b6
b7C

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Thursday, June 07, 2007 2:13 PM
To: [redacted] (OS) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OS) (FBI); [redacted] (OTD) (FBI)
Subject: RE: Tools for upcoming deployment

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

We would love to help put something on there.

[redacted]

Also need the warrant expiration date.

b2
b7E

[redacted]

[redacted]

v/r
J.

CASE INFORMATION
Case ID:
Location:
Date Warrant Signed:
Warrant Expiration Date:
Date Installed/Deployed:
OGC Review and Confirmation

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-24-2008 BY 60322/UCLRP/PJ/EHL

Points of Contact
Case Agent Name, Address and Phone

Tech Agent Name and Phone Number

Equipment Mailing Address and Phone Number

Deployment Technique

Criminal FISA

Install Type

[redacted] Other:

[redacted]

b2
b7E

[redacted]

Applications of Interest

Other Info as known.

[redacted]

[redacted]

b2
b7E

DATA TO BE CAPTURED

[redacted]

b2
b7E

[redacted]

[redacted]

-----Original Message-----

From: [redacted](OTD) (FBI)
Sent: Thursday, June 07, 2007 11:43 AM
To: [redacted](OS) (FBI)
Cc: [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OS) (FBI)
Subject: RE: Tools for upcoming deployment

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b2 b7E

[redacted] For now we can put [redacted]

I would recommend [redacted]

-----Original Message-----
From: [redacted](OS) (FBI)
Sent: Thursday, June 07, 2007 11:18 AM
To: [redacted](OTD) (FBI)
Subject: Tools for upcoming deployment

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6 b7C

Hi [redacted]

[redacted]

I understand that one of the benefits of us being one big happy family is that we can finally utilize our own in-house tools.

That being the case. The case agent would like to [redacted] b2 b7E

Also, what do we need in terms of getting the [redacted] to the case agent?

Thanks

[redacted]

b6 b7C

-----Original Message-----
From: [redacted](OTD) (FBI)
Sent: Thursday, June 07, 2007 9:30 AM
To: [redacted](OS) (FBI)
Cc: [redacted](OS) (FBI); [redacted](OTD) (FBI)
Subject: RE: [redacted]

b2 b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Sorry for the late response. Mon. & Thurs. You know.

[redacted] b2 b7E

-----Original Message-----
From: [redacted](OS) (FBI)
Sent: Tuesday, June 05, 2007 10:14 AM
To: [redacted](OTD) (FBI)
Cc: [redacted](OS) (FBI)
Subject: [redacted]

b6 b7C

b2 b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

H[redacted]

We have an op scheduled for next Thursday, any chance this will be ready for use by then?

[redacted]
SSA [redacted]
Operational Technology Division (OTD)
Cryptologic and Electronic Analysis Unit (CEAU)
[redacted](cell)
desk)
fax)

b6
b7C

-----Original Message-----
From: [redacted](OTD) (FBI)
Sent: Monday, June 04, 2007 1:42 PM
To: [redacted](OTD) (FBI)
Cc: [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted]OTD) (FBI); [redacted](OS) (FBI); [redacted](OS) (CON)
Subject: Windows [redacted]

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b7E

[redacted]is in a limited but usable state.

[redacted]

Capabilities:

[redacted]

b2
b7E

Sending to test today, but could pull something together for a case if emergency.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

4.2

b2
b7E
b1

(S) 4.2.1

Description: Collects any or all of the following:

Features:

b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Several predefined configurations

View Data
Limitations
Types of Cases supported -
Legal Authorization Required
Over-collection Safeguards

DATE: 11-24-2008
CLASSIFIED BY 60322/UCLRP/PJ/EHL
REASON: 1.4 (c)
DECLASSIFY ON: 11-24-2033

4.2.2

b2
b7E

Features

View Data
Limitations

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI) b6 b7C
Sent: Monday, October 15, 2007 2:35 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (CON)
Subject: RE: Inspection questions

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

DATE: 11-24-2008
CLASSIFIED BY 60322/UCLRP/PJ/EHL
REASON: 1.4 (c)
DECLASSIFY ON: 11-24-2033
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted] (OTD) (FBI) b6 b7C
Sent: Thursday, October 11, 2007 4:36 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: Inspection questions

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Gents,

Please provide input on the following:
3-4 examples for each would be great. I'll compile and forward them.

Thanks,
[redacted] b6 b7C

1) Identify the five most significant accomplishments (not investigative cases) for the Unit during the inspection period and provide a narrative assessment of the impact of these accomplishments upon the Unit's mission.

[redacted] b1

2) List by title and file number the ten most significant investigations managed by the unit during the inspection period. Provide a narrative summary for each case, its impact, and the contribution made to the investigation by the unit.

(S [redacted] b1

(S)

(S)

(S

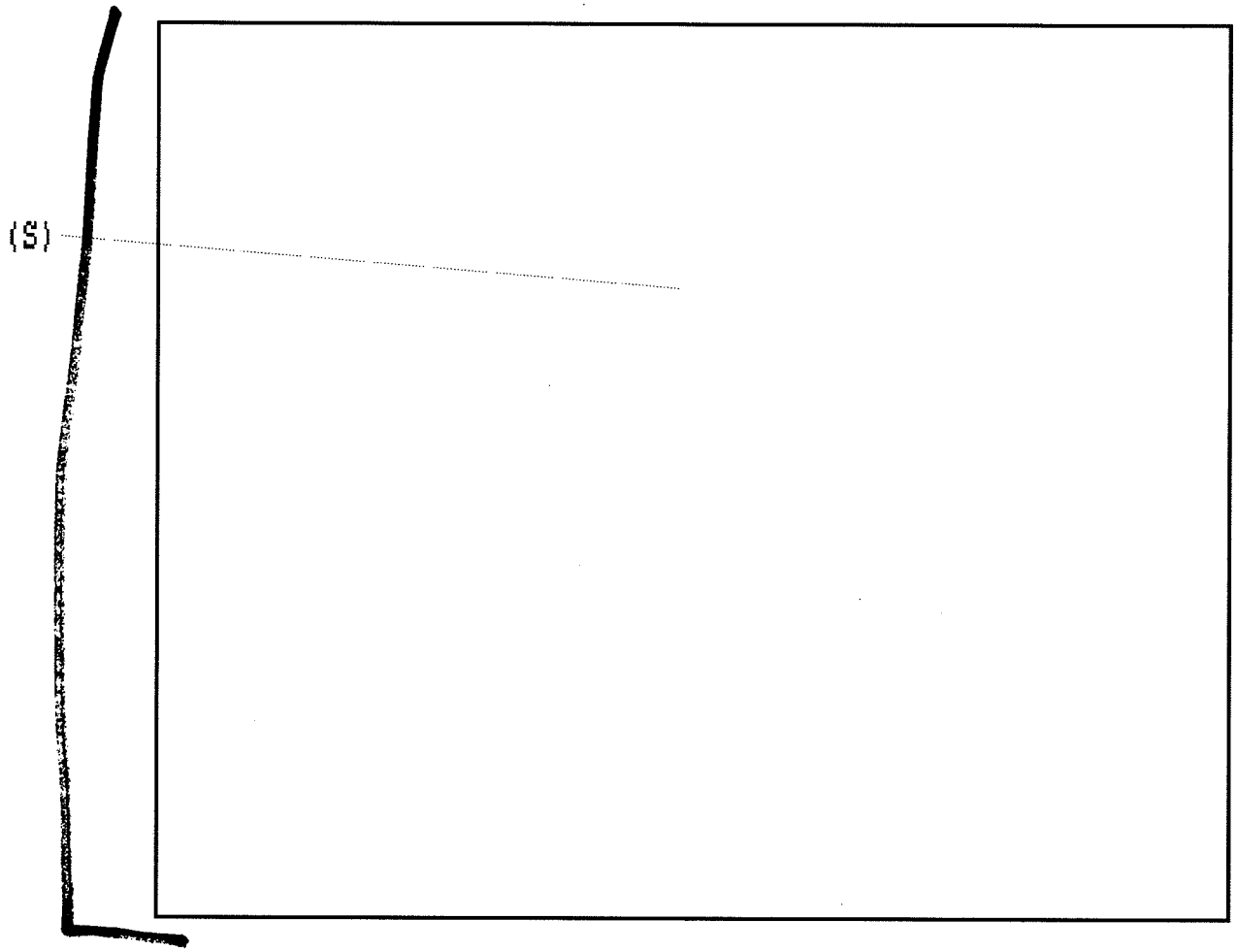
3) Identify at least seven of the most significant liaison contacts (a mix of domestic and international contacts preferred, if possible) of the unit; describe the nature and extent of liaison activities with each agency; explain how this contact advances the unit's mission and helps the unit achieve its goals and objectives.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

b1
b2
b7E



SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

From: [redacted] (OTD) (FBI)
Sent: Friday, June 29, 2007 11:42 AM
To: [redacted] (OTD) (FBI)
Subject: RE: [redacted]

b6
b7C

b2
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

~~SECRET~~

An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol

Salman A. Baset and Henning Schulzrinne
Department of Computer Science
Columbia University, New York NY 10027
{salman,hgs}@cs.columbia.edu

September 15, 2004

ABSTRACT

Skype is a peer-to-peer VoIP client developed by KaZaa in 2003. Skype claims that it can work almost seamlessly across NATs and firewalls and has better voice quality than the MSN and Yahoo IM applications. It encrypts calls end-to-end, and stores user information in a decentralized fashion. Skype also supports instant messaging and conferencing.

This report analyzes key Skype functions such as login, NAT and firewall traversal, call establishment, media transfer, codecs, and conferencing under three different network setups. Analysis is performed by careful study of Skype network traffic.

Categories and Subject Descriptors

C.2.2 [**Computer-Communication Networks**]: Network Protocols—*Applications*

General Terms

Algorithms, Design, Measurement, Performance, Experimentation, Security,

Keywords

Peer-to-peer (p2p), Voice over IP (VoIP), Super Node (SN), Internet telephony, conferencing

1. INTRODUCTION

Skype is a peer-to-peer VoIP client developed by KaZaa [17] that allows its users to place voice calls and send text messages to other users of Skype clients. In essence, it is very similar to the MSN and Yahoo IM applications, as it has capabilities for voice-calls, instant messaging, audio conferencing, and buddy lists. However, the underlying protocols and techniques it employs are quite different.

Like its file sharing predecessor KaZaa, Skype is an overlay peer-to-peer network. There are two types of nodes in this overlay network, ordinary hosts and super nodes (SN). An ordinary host is a Skype application that can be used to place voice calls and send text messages. A super node is an ordinary host's end-point on the Skype network. Any node with a public IP address having sufficient CPU, memory, and network bandwidth is a candidate to become a super node. An ordinary host must connect to a super node and must register itself with the Skype login server for a successful login. Although not a Skype node itself, the Skype login server is an important entity in the Skype network. User names and passwords are stored at the login server. User authentication at login is also done at this server. This server also ensures that Skype login names are unique across the Skype name space. Figure 1 illustrates the relationship between ordinary hosts, super nodes and login server.

Apart from the login server, there is no central server in the Skype network. Online and offline user information is stored and propagated in a decentralized fashion and so are the user search queries.

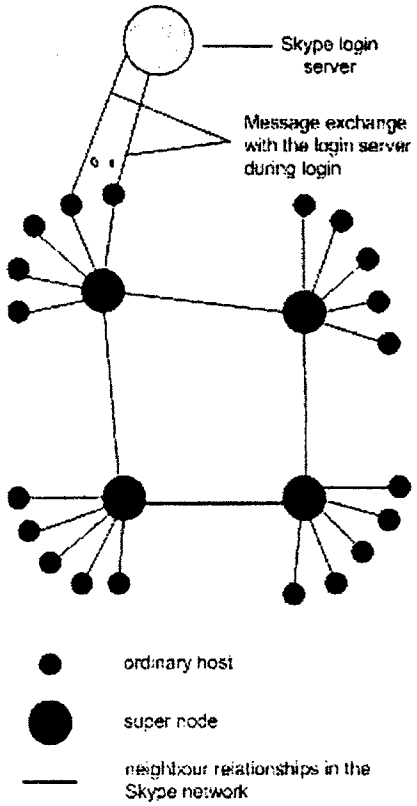


Figure 1. Skype Network. There are three main entities: supernodes, ordinary nodes, and the login server.

NAT and firewall traversal are important Skype functions. We believe that each Skype node uses a variant of STUN [1] protocol to determine the type of NAT and firewall it is behind. We also believe that there is no global NAT and firewall traversal server because if there was one, the Skype node would have exchanged

traffic with it during login and call establishment in the many experiments we performed.

The Skype network is an overlay network and thus each Skype client (SC) should build and refresh a table of reachable nodes. In Skype, this table is called host cache (HC) and it contains IP address and port number of super nodes. It is stored in the Windows registry for each Skype node.

Skype claims to have implemented a '3G P2P' or 'Global Index' [2] technology (Section 4.3), which is guaranteed to find a user if that user has logged in the Skype network in the last 72 hours.

Skype uses wideband codecs which allows it to maintain reasonable call quality at an available bandwidth of 32 kb/s. It uses TCP for signaling, and both UDP and TCP for transporting media traffic. Signaling and media traffic are not sent on the same ports.

The rest of this report is organized as follows. Section 2 describes key components of the Skype software and the Skype network. Section 3 describes the experimental setup. Section 4 discusses key Skype functions like startup, login, user search, call establishment, media transfer and codecs, and presence timers. Flow diagrams based on actual network traffic are used to elaborate on the details. Section 5 discusses conferencing. Section 6 discusses other experiments.

2. KEY COMPONENTS OF THE SKYPE SOFTWARE

A Skype client listens on particular ports for incoming calls, maintains a table of other Skype nodes called host cache, uses wideband codecs, maintains a buddy list, encrypts messages end-to-end, and determines if it is behind a NAT or a firewall. This section discusses these components and functionalities in detail.

2.1 Ports

A Skype client (SC) opens a TCP and a UDP listening port at the port number configured in its connection dialog box. SC randomly chooses the port number upon installation. In addition, SC also opens TCP listening ports at port number 80 (HTTP port), and port number 443 (HTTPS port). Unlike many Internet protocols, like SIP [5] and HTTP [6], there is no default TCP or UDP listening port. Figure 15 shows a snapshot of the Skype connection dialog box. This figure shows the ports on which a SC listens for incoming connections.

2.2 Host Cache

The host cache (HC) is a list of super node IP address and port pairs that SC builds and refreshes regularly. It is the most critical part to the Skype operation. At least one valid entry must be present in the HC. A valid entry is an IP address and port number of an online Skype node. A SC stores host cache in the Windows registry at HKEY_CURRENT_USER / SOFTWARE / SKYPE / PHONE / LIB / CONNECTION / HOSTCACHE. After running a SC for two days, we observed that HC contained a maximum of 200 entries. Host and peer caches are not new to Skype. Chord [19], another peer-to-peer protocol has a finger table, which it uses to quickly find a node.

2.3 Codecs

The white paper [7] observes that Skype uses iLBC [8], iSAC [9], or a third unknown codec. GlobalIPSound [10] has implemented the iLBC and iSAC codecs and their website lists Skype as their partner. We believe that Skype uses their codec implementations. We measured that the Skype codecs allow frequencies between 50-8,000 Hz to pass through. This frequency range is the characteristic of a wideband codec.

2.4 Buddy List

Skype stores its buddy information in the Windows registry. Buddy list is digitally signed and encrypted. The buddy list is local to one machine and is not stored on a central server. If a user uses SC on a different machine to log onto the Skype network, that user has to reconstruct the buddy list.

2.5 Encryption

The Skype website [13] explains: "Skype uses AES (Advanced Encryption Standard) – also known as Rijndel – which is also used by U.S. Government organizations to protect sensitive information. Skype uses 256-bit encryption, which has a total of 1.1×10^{77} possible keys, in order to actively encrypt the data in each Skype call or instant message. Skype uses 1536 to 2048 bit RSA to negotiate symmetric AES keys. User public keys are certified by Skype server at login."

2.6 NAT and Firewall

We conjecture that SC uses a variation of the STUN [1] and TURN [18] protocols to determine the type of NAT and firewall it is behind. We also conjecture that SC refreshes this information periodically. This information is also stored in the Windows registry.

Unlike its file sharing counter part KaZaa, a SC cannot prevent itself from becoming a super node.

3. EXPERIMENTAL SETUP

All experiments were performed for Skype version 0.97.0.6. Skype was installed on two Windows 2000 machines. One machine was a Pentium II 200MHz with 128 MB RAM, and the other machine was a Pentium Pro 200 MHz with 128 MB RAM. Each machine had a 10/100 Mb/s Ethernet card and was connected to a 100 Mb/s network.

We performed experiments under three different network setups. In the first setup, both Skype users were on machines with public IP addresses; in the second setup, one Skype user was behind port-restricted NAT; in the third setup, both Skype users were behind a port-restricted NAT and UDP-restricted firewall. NAT and firewall machines ran Red Hat Linux 8.0 and were connected to 100 Mb/s Ethernet network.

Ethereal [3] and NetPeeker [4] were used to monitor and control network traffic, respectively. NetPeeker was used to tune the bandwidth so as to analyze the Skype operation under network congestion.

For each experiment, the Windows registry was cleared of any Skype entries and Skype was reinstalled on the machine.

All experiments were performed between February and April, 2004.

4. SKYPE FUNCTIONS

Skype functions can be classified into startup, login, user search, call establishment and tear down, media transfer, and presence messages. This section discusses each of them in detail.

4.1 Startup

When SC was run for the first time after installation, it sent a HTTP 1.1 GET request to the Skype server (skype.com). The first line of this request contains the keyword 'installed'.

During subsequent startups, a SC only sent a HTTP 1.1 GET request to the Skype server (skype.com) to determine if a new version is available. The first line of this request contains the keyword 'getlatestversion'.

See the Appendix for complete messages.

4.2 Login

Login is perhaps the most critical function to the Skype operation. It is during this process a SC authenticates its user name and password with the login server, advertises its presence to other peers and its buddies, determines the type of NAT and firewall it is behind, and discovers online Skype nodes with public IP addresses. We observed that these newly discovered nodes were used to maintain connection with the Skype network should the SN to which SC was connected became unavailable.

4.2.1 Login Process

As discussed in Section 2, the HC must contain a valid entry for a SC to be able to connect to the Skype network. If the HC was filled with only one invalid entry, SC could not connect to the Skype network and reported a login failure. However, we gained useful insights in the Skype login process by observing the message flow between SC and this invalid HC entry. The experimental setup and observations for the login process are described below.

First, we flushed the SC host cache and filled it with only one entry which was the IP address and port number of a machine on which no Skype client was running. The SC was then started and a login attempt was made. Since HC had an invalid entry, SC could not connect to the Skype network. We observed that the SC first sent a UDP packet to this entry. If there was no response after roughly five seconds, SC tried to establish a TCP connection with this entry. It then tried to establish a TCP connection to the HC IP address and port 80 (HTTP port). If still unsuccessful, it tried to connect to HC IP address and port 443 (HTTPS port). SC then waited for roughly 6 seconds. It repeated the whole process four more times after which it reported a login failure.

We observed that a SC must establish a TCP connection with a SN in order to connect to the Skype network. If it cannot connect to a super node, it will report a login failure.

Most firewalls are configured to allow outgoing TCP traffic to port 80 (HTTP port) and port 443 (HTTPS port). A SC behind a firewall, which blocks UDP traffic and permits selective TCP traffic, takes advantage of this fact. At login, it establishes a TCP connection with another Skype node with a public IP address and port 80 or port 443.

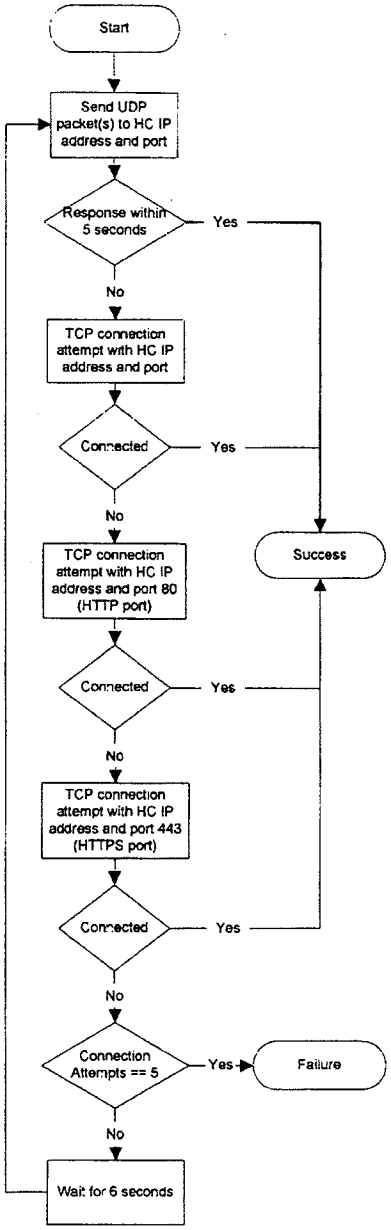


Figure 2. Skype login algorithm. Only one entry is present in the HC. If there is more than one entry, SC sends UDP packets to them before attempting a TCP connection. Authentication with the login server is not shown.

4.2.2 Login Server

After a SC is connected to a SN, the SC must authenticate the user name and password with the Skype login server. The login server is the only central component in the Skype network. It stores Skype user names and passwords and ensures that Skype user names are unique across the Skype name space. SC must

authenticate itself with login server for a successful login. During our experiments we observed that SC always exchanged data over TCP with a node whose IP address was 80.160.91.11. We believe that this node is the login server. A reverse lookup of this IP address retrieved NS records whose values are **ns14.inet.tele.dk** and **ns15.inet.tele.dk**. It thus appears from the reverse lookup that the login server is hosted by an ISP based in Denmark.

4.2.3 Bootstrap Super Nodes

After logging in for the first time after installation, HC was initialized with seven IP address and port pairs. We observed that upon first login, HC was always initialized with these seven IP address and port pairs except for a rare random occurrence. In the case where HC was initialized with more than seven IP addresses and port pairs, it always contained those seven IP address and port pairs. It was with one of these IP address and port entries a SC established a TCP connection when a user used that SC to log onto the Skype network for the first time after installation. We call these IP address and port pairs bootstrap super nodes. Figure 16 shows a snapshot of the host cache of the SC that contains IP address and port numbers of these bootstrap super nodes. These IP address and port pairs and their corresponding host names obtained using a reverse lookup are:

IP address:port	Reverse lookup result
66.235.180.9:33033	sls-cb10p6.dca2.superb.net
66.235.181.9:33033	ip9.181.susc.suscom.net
80.161.91.25:33033	0x50a15b19.boanxx15.adsl-dhcp.tele.dk
80.160.91.12:33033	0x50a15b0c.albnxx9.adsl-dhcp.tele.dk
64.246.49.60:33033	rs-64-246-49-60.ev1.net
64.246.49.61:33033	rs-64-246-49-61.ev1.net
64.246.48.23:33033	ns2.ev1.net

From the reverse lookup, it appears that bootstrap SNs are connected to the Internet through four ISPs. Superb [14], Suscom [15], ev1.net [16] are US-based ISPs.

After installation and first time startup, we observed that the HC was empty. However upon first login, the SC sent UDP packets to at least four nodes in the bootstrap node list. Thus, either bootstrap IP address and port information is hard coded in the SC, or it is encrypted and not directly visible in the Skype Windows registry, or this is a one-time process to contact bootstrap nodes. We also observed that if the HC was flushed after the first login, SC was unable to connect to the Skype network. These observations suggest that we perform separate experiments to analyze the first-time and subsequent login processes.

4.2.4 First-time Login Process

The SC host cache was empty upon installation. Thus, a SC must connect to well known Skype nodes in order to log on to the Skype network. It does so by sending UDP packets to some bootstrap super nodes and then waits for their response over UDP for some time. It is not clear how SC selects among bootstrap SNs to send UDP packets to. SC then established a TCP connection with the bootstrap super node that responded. Since more than one node could respond, a SC could establish a TCP connection with more than one bootstrap node. A SC, however, maintains a TCP connection with at least one bootstrap node and may close TCP connections with other nodes. After exchanging some packets with SN over TCP, it then perhaps acquired the address of the login server (80.160.91.11). SC then establishes a TCP connection with the login server, exchanges authentication information with it, and finally closes the TCP connection. The initial TCP data exchange with the bootstrap SN and the login server shows the existence of a challenge-response mechanism.

The TCP connection with the SN persisted as long as SN was alive. When the SN became unavailable, SC establishes a TCP connection with another SN.

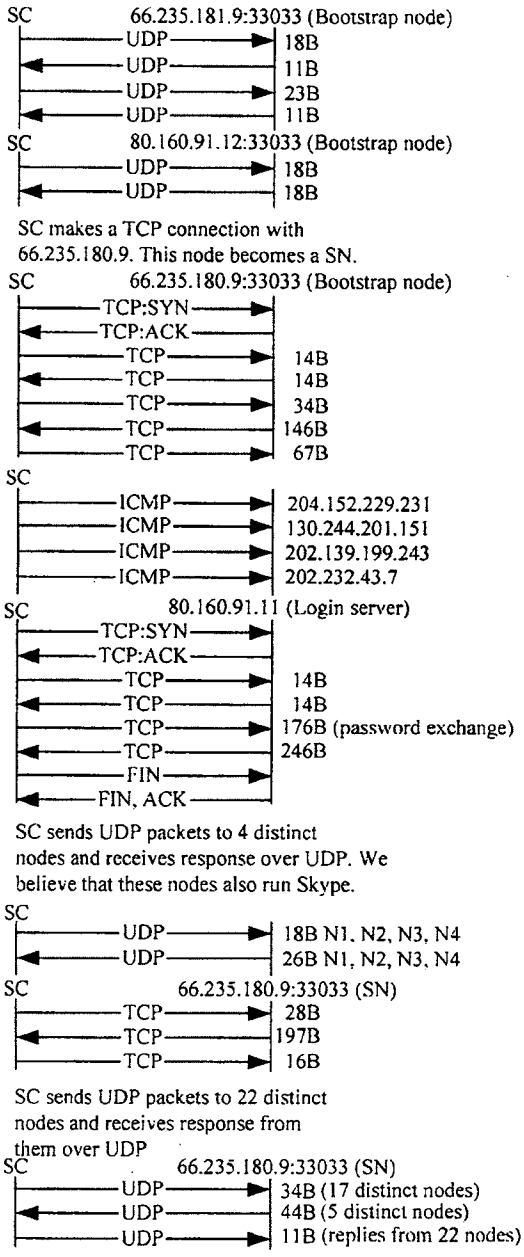
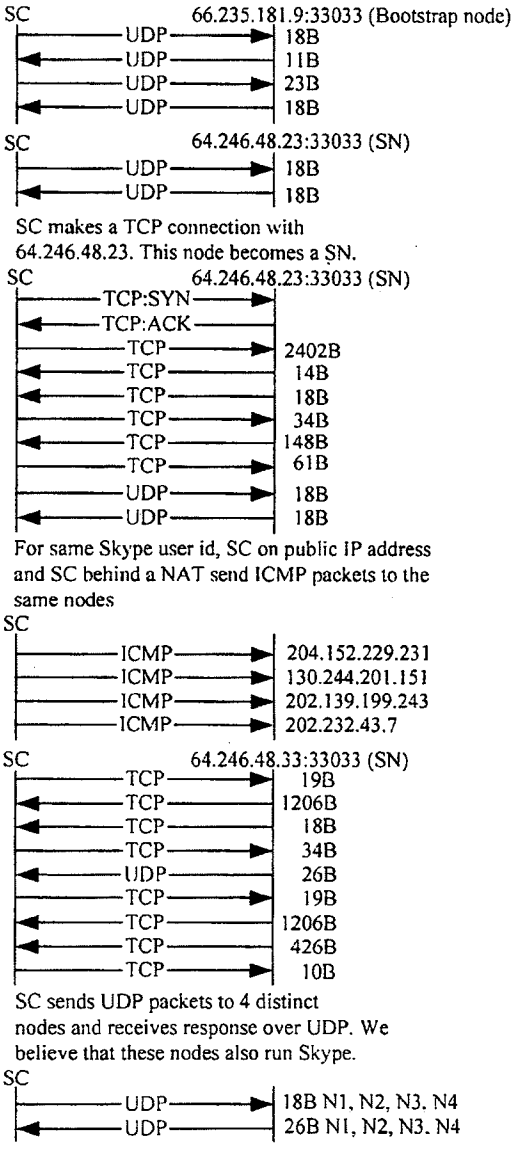


Figure 3. Message flow for the first login after installation for SC on a public IP address. 'B' stands for bytes and 'N' stands

for node. SYN and ACK packets are shown to indicate who initiated TCP connection. Message flows are not strictly according to time. Messages have been grouped together to provide a better picture. Message size corresponds to size of TCP or UDP payload. Not all messages are shown.

For the login process, we observed message flow for the same Skype user id for the three different network setups described in Section 3.

The message flow for the first-time login process for a SC running on a machine with public IP address is shown in Figure 3. The total data exchanged between SC, SN, login server, and other nodes during login is about 9 kilobytes.



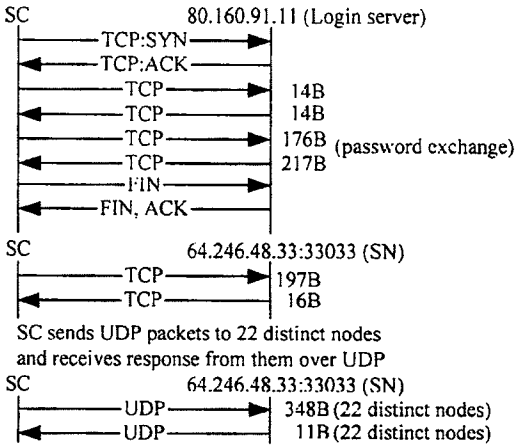


Figure 4. Message flow for first login after installation for SC behind a simple NAT. 'B' stands for bytes and 'N' stands for node. SYN and ACK packets are shown to indicate who initiated TCP connection. Message flows are not strictly according to time. Messages have been grouped together to provide a better picture. Message size corresponds to size of TCP or UDP payload. Not all messages are shown in the message flow.

For a SC behind a port-restricted NAT, the message flow for login was roughly the same as for a SC on a public IP address. However, more data was exchanged. On average, SC exchanged 10 kilobytes of data with SN, login server, and other Skype nodes. The message flow is shown in Figure 4.

A SC behind a port-restricted NAT and a UDP-restricted firewall was unable to receive any UDP packets from machines outside the firewall. It therefore could send and receive only TCP traffic. It had a TCP connection with a SN and the login server, and it exchanged information with them over TCP. On average, it exchanged 8.5 kilobytes of data with SN, login server, and other Skype nodes. The message flow is shown in Figure 5.