

The logo for XKEYSCORE, featuring the word "KEYSCORE" in a bold, blue, 3D-style font with a white outline. The letters are set against a large, stylized grey "X" that has a 3D effect with black and white shading. The background of the slide is a blue gradient with a faint globe and binary code.

VOIP in XKEYSCORE

March 2009

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20291123

DERIVED FROM: NSA/CSSM 1-52



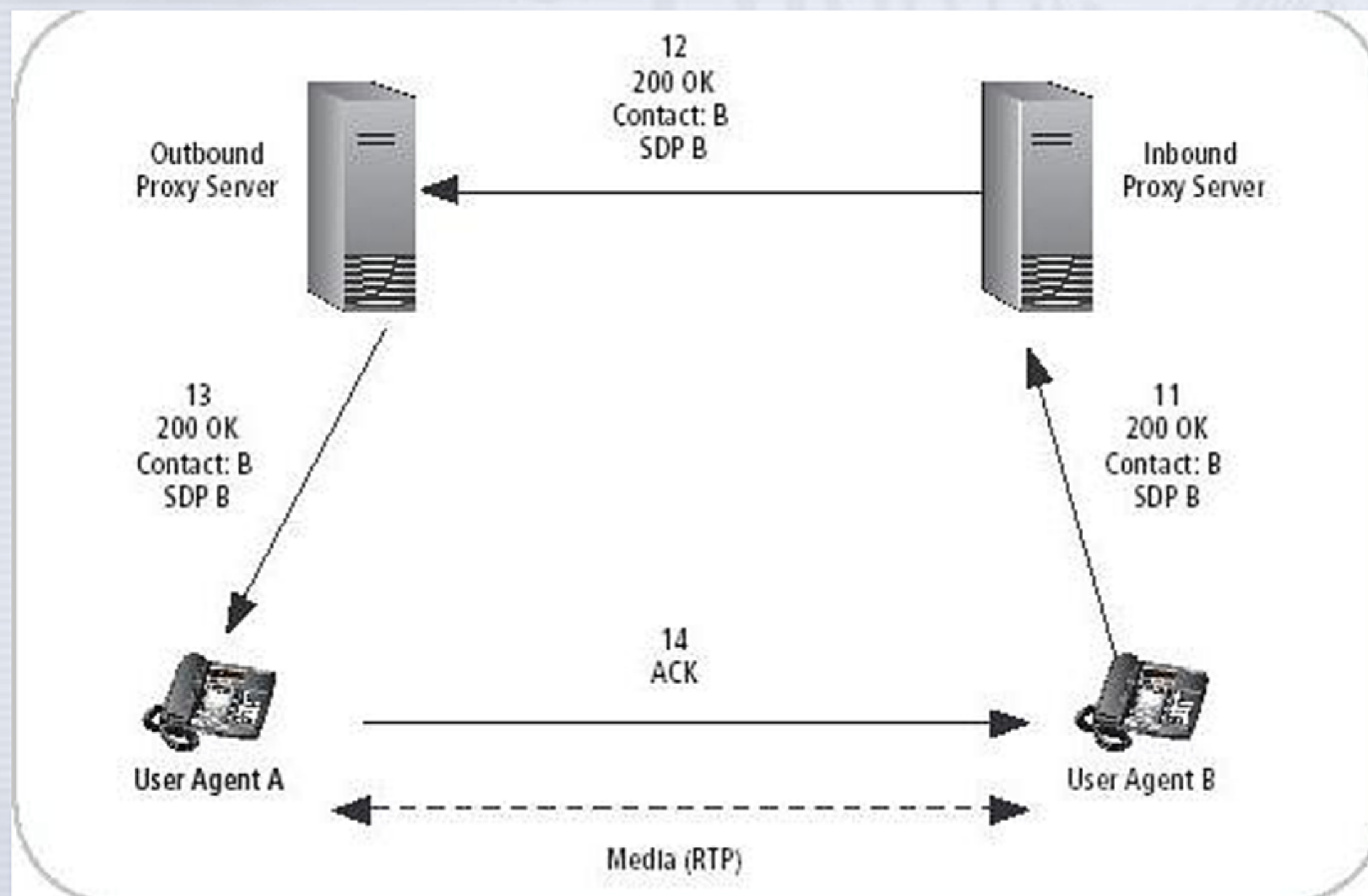
Protocols

- Signaling/setup/control
 - SIP (Session Initiation Protocol)
 - H323
 - Skinny
 - Clarent
 - Yahoo proprietary
- Data - voice, fax, video
 - RTP (Real-time Transport Protocol)



The Problem

- Setup and data may take different routes
- Different routes may be collected at different sites
- Routes may change



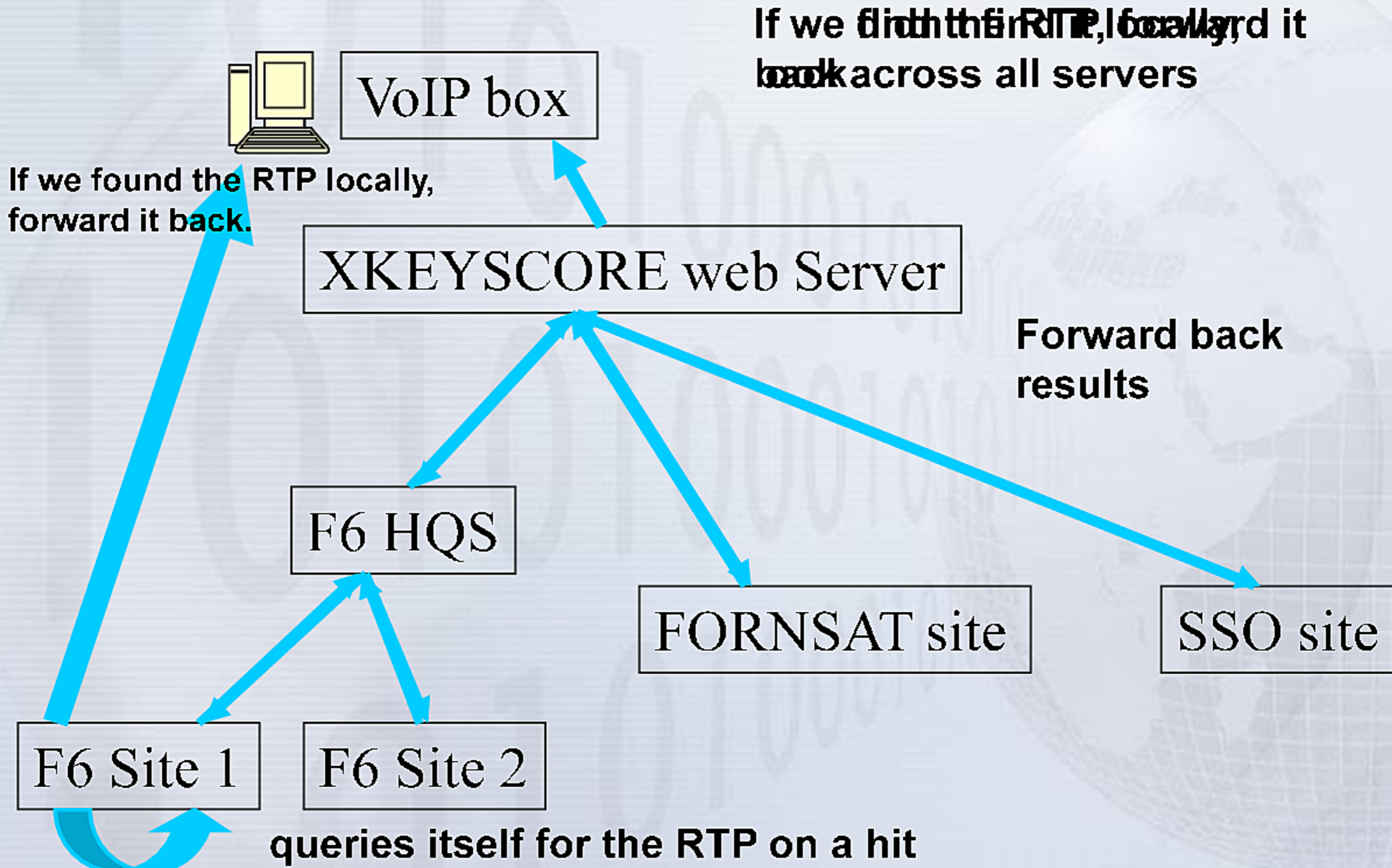


XKS Solution

1. Local site XKS identifies VOIP setup involving a tasked target
2. Local XKS queries itself for corresponding RTP data
3. If the local query fails, it is passed back to HQS for a cross-site query across the entire XKS network
4. Forward hits to NUCLEON and generate summary reports



XKS Solution





VOIP Hits

Use this to find data for which...

- There was a dictionary hit on the VOIP signaling (TRAFFICTHIEF, CADENCE, OCTAVE, MARINA, UTT)

... AND ...

- We were able to find the RTP corresponding to the signaling information

VOIP Hits



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//Z032011

XKEYSCORE

Welcome: oper

[switch users](#)

[Home](#)
[Admin](#)
[Users](#)
[Workflow Central](#)
[Search](#)
[Results](#)
[Statistics](#)
[Preferences](#)
[Help](#)

Navigation Menu

- Search
 - Classic
 - Common
 - Dictionary Hits
 - File Transfer
 - MultiSearch
 - Network Management
 - Search Wizard
 - UserActivity
 - VoIP
 - Hits**
 - Sigdev
 - Wireless

Search: Voip

Query Name: Justification: Additional Justification: Miranda Number: Datetime: Start: Stop: Email: From Email: To Name: From Name: To Phone Number: From Phone Number: To Country Phone Number: From Country Phone Number: To Tasking Type: Tasking Value: Dictionary: Category: Priority: Target: Description: Contacts:



VOIP Hits - Search Form

- User/target information
 - Email
 - Name
 - Phone number
 - IP address
 - Country code
- Content information
 - Content type (audio, video, image)
 - Control type (SIP, H323, skinny, clarent)
 - Fingerprints - may indicate specific VOIP devices



VOIP Hits - Results

ID ▲	Datetime	Datetime End	Content	From Email	From Name	From Phone#	From Country#	To Email
91	2009-03-03 05:05:28	2009-03-03 05:08:42		d @yahoo	"d "			h @yah
92	2009-03-03 06:41:22	2009-03-03 06:42:33		a @yahoo	"a "			s @yahoo
93	2009-03-03 09:39:09	2009-03-03 09:48:05		b @yahoo	b			s @yahoo
94	2009-03-03 09:36:01	2009-03-03 09:37:09		b @yahoo	b			s @yahoo
95	2009-03-03 10:02:31	2009-03-03 10:02:52		b @yahoo	b			s @yahoo
96	2009-03-03 12:57:27	2009-03-03 12:57:41		o @yahoo	"o "			g @yah
97	2009-03-03 05:05:28	2009-03-03 05:08:42		d @yaho	"d "			h @ya
98	2009-03-03 06:41:22	2009-03-03 06:42:33		a @yahoo	"a "			s @yahoo
99	2009-03-03 07:50:18	2009-03-03 07:50:18		0092 @ .23		9234	pakistan	6661 @
100	2009-03-03 07:50:18	2009-03-03 08:04:15		0092 @ .23		9234	pakistan	6661 @

VOIP Hits - RTP Viewer



Actions Reports View

State	ID	Datetime	Datetime End	Content	From Et
	91	2009-03-03 05:05:28	2009-03-03 05:08:42		d
	92	2009-03-03 06:41:22	2009-03-03 06:42:33		a
	93	2009-03-03 09:39:09	2009-03-03 09:48:05		b
	94	2009-03-03 09:36:01	2009-03-03 09:37:09		b
	95	2009-03-03 10:02:31	2009-03-03 10:02:52		b

X-KEYSCORE C2C Session Viewer

Session 1 of 160

Datetime	Case Notation	From IP	To IP	From Port	To Port	Pro
2009-03-03 05:05:28	0000000	.61.149	.11.214	10122	8052	UD

Session Header (3) Meta (4)

Formatter: AUTO

Send to: Download Session

Mode: Snippet

Options

Search Content:

Enter text to search

Quick Clicks

- Session
- One-Click Searches
 - Find opposite side of session
 - .61.149:10122 -
 - .11.214:8052
 - Find traffic on
 - .11.214
 - .61.149
 - Find application
 - multimedia/rtp/g729
 - Find fingerprint
 - region/

AUTO FORMATTER: app_id= multimedia/rtp/g729 Viewer= RTP formatter. Info=

Extracting RTP data...

ssrc	# packets	% packets	# bytes	% bytes	min ts	max ts	min seq	max seq
39c4	9733	100.0%	194650	100.0%	1895262977	1896820097	0	65535
payload	# packets	% packets	# bytes	% bytes	min ts	max ts	min seq	max seq
g729	9733	100.0%	194650	100.0%	1895262977	1896820097	0	65535

Number of bad sequence numbers=2

Decoding media...

```
39c4      g729: raw decoded wav decoded au [194.7 sec] audio processing
combined g729: raw decoded wav decoded au [9.3 sec] audio processing
00000000 g729: raw decoded wav decoded au [0.0 sec] audio processing
```



VOIP Hits - audio

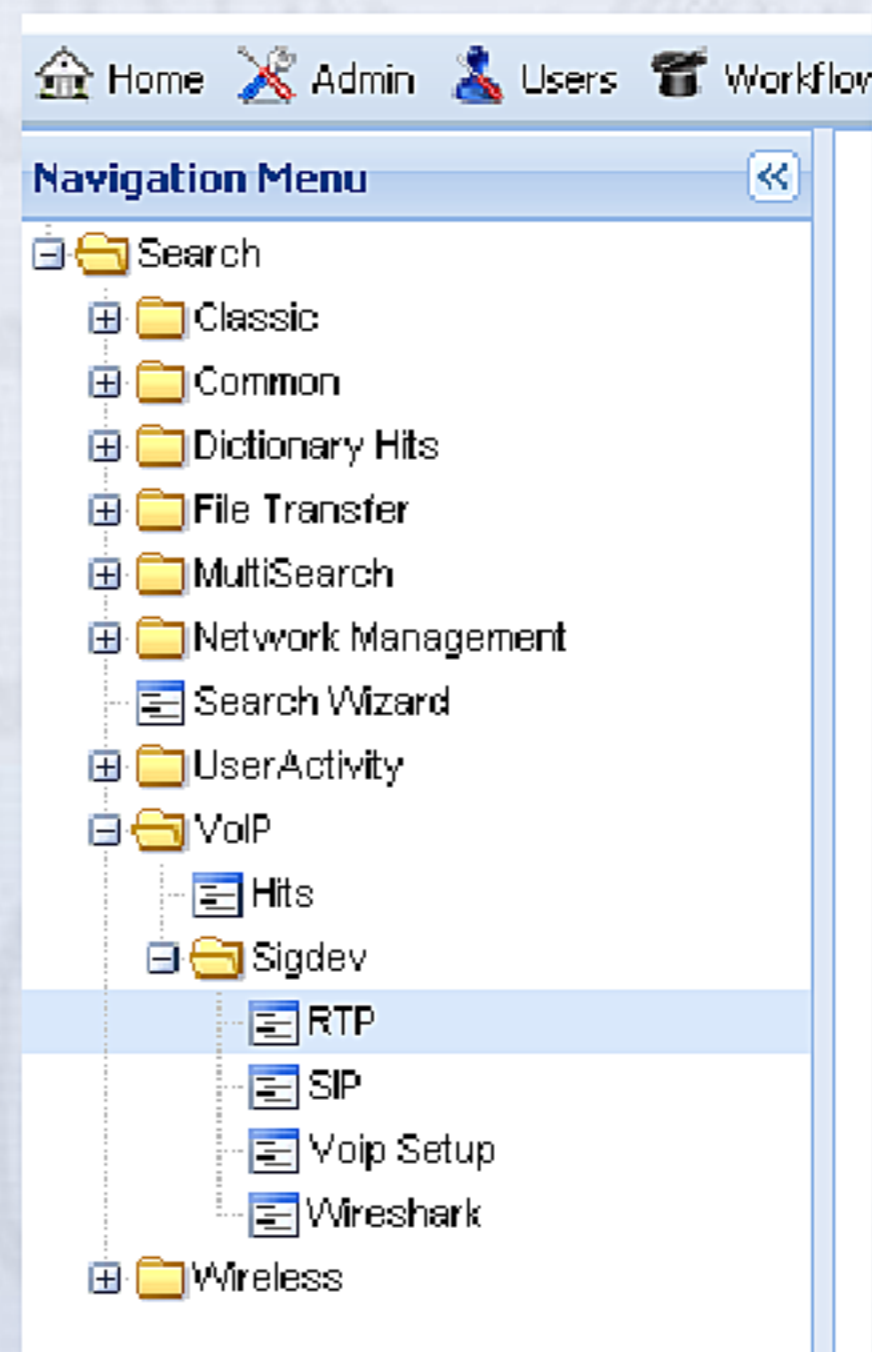
A screenshot of a Windows XP desktop environment. In the foreground, a media player window titled 'Now Playing' is open. The main display area shows a large, glowing cyan CD icon. Above the CD, the text 'get_session_new.php' is displayed. To the right of the CD, there is a smaller image of a musical note and the filename 'get_session_new.php'. Below the note image, the filename 'get_session_new.php' is listed with a duration of '3:14'. At the bottom of the player, a progress bar shows the current time as '00:11' out of a 'Total Time: 3:14'. The status bar at the bottom of the window indicates 'Playing' and 'Ambience : Bubble'. On the left side of the player, a vertical menu contains options: 'Now Playing', 'Media Guide', 'Copy from CD', 'Media Library', 'Radio Tuner', 'Copy to CD or Device', 'Premium Services', and 'Skin Chooser'. In the background, a file explorer window is partially visible, showing a list of files with columns for 'Date' and 'Time'. The desktop taskbar at the bottom shows the Start button, several application icons, and the system tray with a clock and volume icons.



VOIP Sigdev

Use these search forms to find other VOIP not included in the VOIP Hits

- RTP
- SIP
- VOIP Setup
- Wireshark





Questions?

- Contact the team:
 - xkeyscore@nsa.ic.gov
 - <http://xkeyscore.██████████> (go xkeyscore)

- Primary POCs for VOIP:
 - ██████████@nsa.ic.gov
 - ██████████@nsa.ic.gov