



CNE Analysis in XKEYSCORE

15 October 2009

xkeyscore@nsa.ic.gov
([REDACTED]@nsa.ic.gov)



These slides are classified
TS//SI//REL FVEY in their entirety

data indicated as more highly controlled has been filtered out.



CNE Basics

- Tao is a collector
 - analogous to field site
- Various formats based on collection “equipment”
 - OLYMPUS vs UNITEDRAKE :: WC vs TU...
- SRI plus content produces “sessions”
 - dnt payload format
- Significant overlap with passive, especially in terms of collected files
 - office, pdf, ...
- Much unique opportunity
 - Config files, registry, network information,...
- Beginning to feed standard analytic tools



CNE Analytic Projects

- PINWALE (storage/legacy)
- TUNINGFORK (aggregate data views and tasking/legacy)
- XKEYSCORE (discovery+)
- TURBOCHASER/MARINA (profiles [machine and user], future tasking)
- JOLLYROGER/TREASUREMAP (networks)
- TURBINE/PRESSUREWAVE/MAD (future)



Current XKS-CNE Data

- US-3101B, C, D, E, F, L, M
 - UNITEDRAKE
 - TUCKER
 - OLYMPUS
 - EXPANDINGPULLY (formatting issues)
 - UNIX (very little, poorly formatted)
 - *Not FISA, Not ECI*
- Data retention from 29 January (many projects not available until 15 May)



CNE Related Searches

A “typical” day’s CNE results



Selecting all tables generated between '2009-9-22 00:00:00' and '2009-9-23 00:00:00'

Pulling hit data from xks-central.corp.nsa.ic.gov

30 distinct users found 13998 results in 60 separate searches

QUERY RESULTS (ad-hoc):

userxxx email_addresses 22/10421 Iran NPS Domains userxxx_0808493001253628218_1
f652856 document_metadata 11/1053 f652856_0 f652856_0631781001253611176_1
useryyy tech 2/2 Iran Tech Search useryyy_0303242001253646149_1

...

Distribution of Searches by type:

email_addresses: 7

extracted_files: 32

full_log: 5

document_metadata: 6

phone_number: 1

tech: 4

registry: 5



XKEYSCORE Searches (live demo)



Full Log (search)

- Often Used Fields:
 - Input Source (Project Name)
 - Application
 - dnt_payload/file,
 - dnt_payload/dirwalk,
 - ...
- Limit to XKS-CNE box if performing a CNE specific search
- Very similar to “CNE” search

XK Search Full Log - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.com.nsa.ic.gov:3443/XKEYSCORE/

Most Visited Smart Bookmarks Signout: Rj YehaURN Mapper XKS-Central DnsPage - X... XK Search... XK Login #4314 (chang...) TLINGFORC NQ: Results H...

This system is audited for USSID 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL // 202320100
XKEYSCORE Welcome crvermi! Log Out

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation menu

- Java Edition
- JavaName
- Classic AIM
- Identity
- CNE
- Cell Logs
- Category DNI
- Cellular DNI
- Cisco Passwords
- DNS
- Document Metadata
- Document Tagging
- Email Addresses
- Extracted File
- Full Log DNI
- HTTP Activity
- IKE Policy
- Juglal and Passwords
- MacBook Metadata
- Classic NZE
- KEYLOGGER
- Network Logs
- PDF Metadata
- OLE/EMM
- PPT VoIP Metadata
- Report
- Phone Number Editor
- RPT API
- REGISTRY
- RTP
- Radio Log
- SEP
- SSL Parser
- Tech Strings in Document
- User Activity

Application: rht (Encryptions) [fulltext]

SIGAD

Casenotation

Session ID (UUID)

Associated Session [fulltext]

Block Number

Data Length

Session Length

Protocol

Tasking ID

Persona ID

External Metadata Fields [fulltext]

Input Occurs

Populate with Field B

Populate with Tree F

This system is audited for USSID 18 and Human Rights Act compliance



Full Log (results)

XK Results - Mozilla Firefox

File Edit View Bookmarks Tools Help

https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/

Most Visited Smart Bookmarks JSignout: R1 Yehia URN Mapper XKEYSCORE DomsPage - XKEYSCORE...

JSignout: R1 SEARCHLIGHT... DomsPage - X... XK Resu... XK Login #4314 (chan... TUNINGFORK NKB: Results https://0.html XKSearch: Fu...

This system is audited for USSID 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108
XKEYSCORE Welcome [Log Out](#)

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation Menu

- XKEYSCORE LAYOUT
- ■ RBGAN
- ■ REGISTRY
- ■ RTP
- ■ Radius Logs
- ■ SP
- ■ SSL Parser
- ■ Tech Strings in Docum...
- ■ User Activity
- ■ WLAN
- ■ Web File Transfer
- ■ Web Proxy
- ■ Wireshark
- + Common
- + Dictionary Hits
- + File Transfer
- + MultiSearch
- + Network Management
- + UserActivity
- + VoIP
- + Wireless
- + Workflow Central
 - ■ Request
 - ■ AllWorkflows
 - ■ All Pending Workflows
 - ■ My Workflows
- + Results

All Previous Results

Help Actions View FILTERS:

Query Name	Actions	Status	Query Type	Num Results	Num DBs	Date
tao_wireless_survey_FP_oct09 (WORKFLOW)	 	finished	full_log	12	1 of 1	2009-

Query Text

```
WHERE datetime >= '2009-10-12 0:00:00' AND datetime <= '2009-10-13 0:00:00' AND ( application = 'dnt_payload/wirelessurvey/' ) AND ( fm_country != 'US' AND fm_...
```

Page 1 of 1 Page Size: 30 Displaying 1 - 1 of 1

This system is audited for USSID 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/results/a/results/formSubmit.do?span=Previous# xks-central.corp.nsa.ic.gov:8443



Results Manipulation

XX Metaviewer: 1 - full log (tau-wireless) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://ks-central.corp.nsa.c.../KEYSCORE/

Most Visited Smart Bookmarks 25onut: R1 veeha URN Mapper XKS-Central DnsPage - X-KEYSC... Signout: R1 SEARCHLIGHT DnsPage - X-KEYSC... X Meta... X login #4314 (chang...) TIMINGFOUR NKB:Results https://10.htm XE Search Fil... Home X-Arch Users Search Workflow Central Results Statistics Tagging Tasking My Account X-KEYSCORE Welcome Log Out

This system is audited for LS91D 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA,AUS,CAN,GBR,NZL

Histogram: Input Source

Clear Selection Histogram of Input Source (Click Bar to Filter)

Input Source Count

Input Source	Count
WXTIDE1173	1
SHADOWQUEST36	2
FOXACID6654	8

Navigation Menu

- Web Privacy
- Wireshark
- Common
- Dictionary Hits
- File Transfer
- MultSearch
- Network Management
- UserActivity
- VoIP
- Wireless
- Workflow Central
- Results
- Archived Results
- Ongoing Results
- Downloads
- All Downloads
- Recent Results
- Previous Results
- Archived Results
- Ongoing Results
- Statistics
- Signal Acquisition
- Link Summarization
- Tagging
- Local Tagging
- Tech Extractor
- Testing
- VoIP Testing
- My Account

1 - full log (tau-wireless)

Help Actions Results View FILTERS

AppID (Fingerprints)	Input Source	Session ID (JUD)	TaskingID	Personnel ID	Ch
dnt_payload/wirelesssurvey	FOXACID6654	#4043ba690			
dnt_payload/wirelesssurvey	WXTIDE1173	#003ba691			
dnt_payload/wirelesssurvey	FOXACID6654	#4043ba690			
dnt_payload/wirelesssurvey	FOXACID6654	#003ba6902			
dnt_payload/wirelesssurvey	FOXACID6654	#0003ba690			
dnt_payload/wirelesssurvey	FOXACID6654	#0003ba691			
dnt_payload/wirelesssurvey	FOXACID6654	#0003ba690			
dnt_payload/wirelesssurvey	SHADOWQUEST36	#049B9F631			
dnt_payload/wirelesssurvey	SHADOWQUEST36	#049B9F434			
dnt_payload/wirelesssurvey	FOXACID6654	#0003ba690			
dnt_payload/wirelesssurvey	FOXACID6654	#0043ba690			

Page 1 of 1 > Page Size: 70 (Max: 100 rows per page) Displaying 1 - 12 of 12

AutoFit Column Width

This system is audited for LS91D 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA,AUS,CAN,GBR,NZL

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

Click Thru

NEW

XKEYSCORE Welcome [REDACTED] Log Out

This system is audited for USFSTB 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA//AUS//CAN//GBR//NZL

Navigation Menu

- Web Proxy
- Wireshark
- Common
- Dictionary Hits
- File Transfer
- MultSearch
- Network Management
- User Activity
- VoIP
- Wireless
- Workflow Central
- Requests
- All Workflows
- All Fencing Workflows
- My Workflows
- Results

 - My Recent Results
 - My Previous Results
 - My Archived Results
 - My Ongoing Results
 - My Downloads
 - All Downloads
 - All Recent Results
 - All Previous Results
 - All Archived Results
 - All Ongoing Results

- Statistics
- Signal Acquisition
- Link Summarization
- Tagging
- Local Tagging
- Text Extractor
- Tooling
- Voice Tooling
- My Account

Histogram Input Source

Clear Selection Histogram of InputSource (Click Bar to Rite)

FOXACADE65A 7
SHADOWWAVE 2
WAYNEEL23 1

1 - full log (tao-wireless)

Fingerprint Match

Query	Count
Query JOLLYROGER	1
Query TLNINGFORK	1

Cancel

Displaying 1 - 12 of 12

Page 1 of 1 Page Size 70 (Max 300 rows per page)

saved_31447#0346604101



Session Viewing (XML Default)

XK Session Viewer - Mozilla Firefox

File Edit View Bookmarks Tools Help

<https://xk-cne.corp.nsa.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session+Viewer&viewUrl=%2F%2FKEYSCORE%2F%2Fmetaviewer%2Fmetadata%2FviewSession.do%3Fid%3D>

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer [from archive]

[< < Session 1 of 2409 | > >] | ⚙ | Read-ahead: On

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2009-09-30 02:04:51	AF.SPDAECAAADTC						793

Session Header (3) Meta (1)

Formatter: AUTO | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

Quick Clicks

- Session
- One-Click Searches
 - Find application
 - dnt_payload/error
 - Find opposite side of sess
 - :0 ->
 - :0

PAYOUT XML

sess format AUTO content.xml FORMATTER AUTO

Using XML formatter

```
<payload:Payload xmlns:payload="urn:payload:dnt">
  <payload:DataType>Error</payload:DataType>
  <payload:Namespace>urn:payload:dnt</payload:Namespace>
  <payload:Version>1.0.7</payload:Version>
  <payload:TimeInfo>
    <payload:TargetTime>2009-09-26T10:52:37</payload:TargetTime>
    <payload:TargetTimeZoneOffset>4.50</payload:TargetTimeZoneOffset>
    <payload:LocalTimeGMT>2009-09-26T06:35:32+00:00</payload:LocalTimeGMT>
  </payload:TimeInfo>
  <payload:Error type="plugin" value="5535B2593" procedureID="-2142175230">
    <payload:Description>UR Error: Plugin Not Found</payload:Description>
    <payload:Version>
      <payload:Major version="1"/>
      <payload:Minor version="4"/>
      <payload:Build version="1"/>
      <payload:Api version="65536"/>
    </payload:Version>
    <payload:Data></payload:Data>
  </payload:Error>
</payload:Payload>
```



Session Viewing (Specialized per payload)

XKEYSCORE - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-one.corp.nsa.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session%20Viewer&rowUrl=%2F%2Fmetaviewer%2Fmetadata%2FviewSession.do%3Fd%3

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE O2O Session Viewer [from archive]

Session 27 of 2409 | Read-ahead: On

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2009-09-30 02:06:32	IR.SPDCYLAADTC						28636

Session Header (3) Meta (1)

Formatter: AUTO | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

Quick Clicks

- Session
- One-Click Searches
 - Find application
 - dnt_payload/dirwalk
 - Find opposite side of session
 - :0 ->
 - :0

AUTO FORMATTER: app_id= dnt_payload/dirwalk Viewer= DNT_PAYLOAD formatter. Info=

DIRECTORY WALK

open all | close all

- C:\Documents and Settings\aviolat_ed\My Documents\My Skype Pictures\
 - Angel Skype.png
 - Architect Skype.png
 - Beach Skype.png
 - Behind Skype.png
 - Business Skype.png
 - Call Me Sweetheart.png
 - Call Me.png
 - Carnival Skype.png
 - Chic Skype.png
 - Christmas Skype.png
 - College Skype.png
 - Desert Skype.png
 - Designer Skype.png
 - Devil Skype.png
 - DIY Skype.png
 - DJ Skype.png
 - Earbud Skype.png
 - Empire Skype.png
 - Fax Skype.png

Session Viewing (CCDF Headers)



The screenshot shows the XK Session Viewer interface within Mozilla Firefox. The title bar reads "XK Session Viewer - Mozilla Firefox". The menu bar includes File, Edit, View, History, Bookmarks, Tools, Help, and a search icon. The address bar displays the URL: "https://xk-cnc.corp.nsa.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session+Viewer&boxId=%2F%2FKEYSCORE%2F%2Fmetaviewer%2Fmetadata%2FviewSession.do%3Fd%3C%3E". A red banner at the top states: "This system is audited for USSID 18 and Human RigHx Act compliance. CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL". Below the banner, the title "X-KEYSCORE C2C Session Viewer [from archive]" is shown. The main content area has a table with columns: Datetime, Case Notation, From IP, To IP, From Port, To Port, Protocol, and Length. One row is visible: "2009-09-30 02:06:32 IR.SPDCYLAADTC" with a length of "28636". At the bottom, tabs for "Session", "Header (3)", and "Meta (1)" are visible, along with buttons for "Selected_Header_Fields", "Raw_Header_(XML)", and "Full_XKS_Header". The status bar at the bottom right shows "FORMATTER" and "AUTO".

Using XML form atts

```
<ccdf sec:classification="TS" sec:secCoi="COMINT" sec:secNetlDissem="00001" sec:SCIcontrols="SI" sec:dedclassification="X1" release="2.5.1">
<signal version="1.0" id="06c855f6-0124-25d7-1f35-0019B9F630E7" policy="ussid18">
  <signalType>Directory Walk</signalType>
  <begin>2009-09-29T17:10:17Z</begin>
  <profile processedBy="SEAGULLFARO">
    <index>
      <msgType>DTN</msgType>
      <tad>IRX</tad>
      <country title="Iran">IRN</country>
    </index>
    <caseNot side="forward">IR_SPDCYLAADTC</caseNot>
  </profile>
  <characteristic id="06c855f6-0124-25d7-1f35-0019B9F630E7">
    <dataLength unit="octets">28636</dataLength>
    <file></file>
  </characteristic>
</signal>
<processingEvent id="06c06e66-0124-3b11-1f4d-0019B9F630E7">
  <processingType>collection</processingType>
  <processingCat>collection</processingCat>
  <provider>
    <covername>SHADOWQUEST35</covername>
    <pddg>12</pddg>
    <sigad>US-3101C</sigad>
  </provider>
  <service name="forwarding">
    <parameter name="Target">000000010001328B</parameter>
    <parameter name="SEAGULLFARO_UUID">06c855f6-0124-25d7-1f35-0019B9F630E7</parameter>
    <parameter name="TransactionID">000000010001328B.5552.29SE1710209.spouter-2-3.0.fns1_2014091_0_1dup</parameter>
    <parameter name="processor">SEAGULLFARO</parameter>
    <parameter name="Seagullfaro Process Time">2009-09-29T17:10:00Z</parameter>
    <parameter name="Signal_Type">Directory Walk</parameter>
  </service>
</processingEvent>
<processingEvent id="06c06e66-0124-3b11-1f4d-0019B9F630E7">
  <processingType>collection</processingType>
  <processingCat>collection</processingCat>
  <provider>
    <covername>SHADOWQUEST35</covername>
    <pddg>12</pddg>
    <sigad>US-3101C</sigad>
  </provider>
  <service name="forwarding">
    <parameter name="Target">000000010001328B</parameter>
    <parameter name="SEAGULLFARO_UUID">06c855f6-0124-25d7-1f35-0019B9F630E7</parameter>
    <parameter name="TransactionID">000000010001328B.5552.29SE1710209.spouter-2-3.0.fns1_2014091_0_1dup</parameter>
    <parameter name="processor">SEAGULLFARO</parameter>
    <parameter name="Seagullfaro Process Time">2009-09-29T17:10:00Z</parameter>
    <parameter name="Signal_Type">Directory Walk</parameter>
  </service>
</processingEvent>
```



Extracted Files-CNE Specific

XK Results - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://ids-central.corp.rsa.ic.gov:8443/XKEYSCORE/

Most Visited Smart Bookmarks JSignout: R1 Veehia URN Mapper XKS-Central DnsPage - X-KEYSC...
 JSignout: R1 SEARCHLIGHT Query DnsPage - X-KEYS XK Results #4314 (change the TUNINGFORK https://j.../10.html XK Results

This system is audited for USSID 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

XKEYSCORE Welcome Log Out

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation Menu

- SSL Parser
- Tech Strings in Do...
- User Activity
- WLAN
- Web File Transfer
- Web Proxy
- Wireshark
- Common
- Dictionary Hits
- File Transfer
- MultiSearch
- Network Management
- UserActivity
- VoIP
- Wireless
- Workflow Central
- Request
- All Workflows
- All Pending Workflows
- My Workflows
- Results
- My Recent Results
- My Previous Results
- My Archived Results
- My Ongoing Results
- My Downloads
- All Downloads
- All Recent Results
- All Previous Results
- All Archived Results
- All Ongoing Results
- Statistics
- Signal Acquisition

All Previous Results

Help Actions View FILTERS:

Query Text	Actions	Status	Query Type	Num DBs	Datetime Submitted
WHERE datetime >= '2009-09-13 00:00:00' AND datetime <= '2009-10-13 23:59:00' AND (ext_extension = 'pot') AND (inout_source = 'DARKHELNET26') AND (application = dn...)	X E	finished	extracted_files	1 of 1	2009-10-13 14:1

Query Text

```
WHERE datetime >= '2009-09-13 00:00:00' AND datetime <= '2009-10-13 23:59:00' AND ( ext_extension = 'pot' ) AND ( inout_source = 'DARKHELNET26' ) AND ( application = dn... )
WHERE datetime >= '2009-09-13 00:00:00' AND datetime <= '2009-10-13 23:59:00' AND ( ext_extension = 'pot' ) AND ( inout_source = 'DARKHELNET36' ) AND ( application = dn... )
WHERE
WHERE
WHERE
WHERE
WHERE
```

jhesse_0 - Mozilla Firefox

File Edit View Bookmarks Tools Help

https://ids-central.corp.rsa.ic.gov:8443/XKEYSCORE/

Most Visited Smart Bookmarks JSignout: R1 Veehia URN Mapper XKS-Central DnsPage - X-KEYSC...
 JSignout: R1 SEARCHLIGHT Query DnsPage - X-KEYS XK Metaviewer... #4314 (change the TUNINGFORK https://j.../10.html XK Results

This system is audited for USSID 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome Log Out

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation Menu

- SSL Parser
- Tech Strings in Do...
- User Activity
- WLAN
- Web File Transfer
- Web Proxy
- Wireshark
- Common
- Dictionary Hits
- File Transfer
- MultiSearch
- Network Management
- UserActivity
- VoIP
- Wireless
- Workflow Central
- Request
- All Workflows
- All Pending Workflows
- My Workflows
- Results
- My Recent Results
- My Previous Results
- My Archived Results
- My Ongoing Results
- My Downloads
- All Downloads
- All Recent Results
- All Previous Results
- All Archived Results
- All Ongoing Results
- Statistics
- Signal Acquisition

jhesse_0

Help Actions Reports View

#	Size	ID	Datetime	Datetime End	Highlights	Pathname	Extension	File Type (MIME Type)
1	85	2009-09-24 03:49:08	2009-09-24 03:49:23	CNE	WLL(CDMA).ppt	.ppt	application/vnd.ms-powerpoint	
2	86	2009-09-24 03:49:08	2009-09-24 03:49:53	CNE	Basics Commands.ppt	.ppt	application/vnd.ms-powerpoint	
3	87	2009-09-24 03:49:18	2009-09-24 03:49:53	CNE	File Permissions.ppt	.ppt	application/vnd.ms-powerpoint	
4	88	2009-09-24 03:49:08	2009-09-24 03:49:53	CNE	File System.ppt	.ppt	application/vnd.ms-powerpoint	
5	89	2009-09-24 03:49:08	2009-09-24 03:49:53	CNE	Shell.ppt	.ppt	application/vnd.ms-powerpoint	
6	90	2009-09-24 03:49:08	2009-09-24 03:49:53	CNE	Text Editor.ppt	.ppt	application/vnd.ms-powerpoint	
7	91	2009-09-24 03:49:08	2009-09-24 03:49:53	CNE	UNIX.ppt	.ppt	application/vnd.ms-powerpoint	
8	92	2009-09-24 03:49:08	2009-09-24 03:49:53	CNE	UNIX.ppt	.ppt	application/vnd.ms-powerpoint	
9	93	2009-09-24 03:49:10	2009-09-24 03:49:43	CNE	DSL Presentation.ppt	.ppt	application/vnd.ms-powerpoint	

Document Metadata – Active/Passive Converged Analysis



XK Metaviewer Iran - Customs and Rail Extracted Docs - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xk-central.corp.iraq.gov:8443/XKEYSCORE

Smart Bookmarks 35grants.RJ Yesterdays Mapper xk-central OnePage - XKEYSCORE...

Signatures.R1 SEARCHLIGHT Query OnePage - XKEYS XK Metaviewer... XKEYSCORE...

This system is audited for UCOD 2.0 and Human Rights Act compliance
XKEYSCORE Welcome Log Out

Home Admin Users Search Workflow Central Results Statistics Tagging Tracking My Account XK Forum Help

Navigation Menu

- SSL Parser
- Tech Strings In Do
- User Activity
- WLAN
- Web File Transfer
- Web Proxy
- Windows
- Common
- Dictionary Lists
- File Transfer
- MultiSearch
- Network Management
- UserActivity
- VoIP
- Wireless
- Workflow Central
- Request
- All Workflows
- All Pending Workflows
- My Workflows
- Results

 - My Recent Results
 - My Previous Results
 - My Archived Results
 - My Ongoing Results
 - My Downloads
 - All Downloads
 - All Recent Results
 - All Previous Results
 - All Archived Results
 - All Undone Results

- Statistics
- Signal Acquisition
- Link Summarization
- Tagging
- Local Tagging
- Tech Extractor
- Tracking
- Help Tracking
- My Account

Iran_CP_Customs_and_Rail_Extra...

Help Options Reports View FILTERS

Highlights	Datetime	Input Source	Document Type	Encrypted	Corrupted	Filename	Extension	Language	Author	Last Author
CNE ↗	2009-10-09 00:19:56	LUTEUSASTRO1	office/word	no	no	H:\ap top drive\USA\Private Index\ doc	doc	ara	Rasool H.Borji	08978
CNE ↗	2009-10-09 00:19:56	LUTEUSASTRO1	office/word	no	no	H:\ap top drive\USA\Private Index\ doc	doc	ara	08970	
CNE ↗	2009-10-09 12:01:01	LUTEUSASTRO1	office/word	no	no	H:\ap top drive\USA\Private Index\ doc	doc	ara	Rasool H.Borji	08978
CNE ↗	2009-10-09 12:01:01	LUTEUSASTRO1	office/word	no	no	H:\ap top drive\USA\Private Index\ doc	doc	ara	08970	
	2009-10-12 17:16:15		office/word	no	no	3897.doc	doc	ara fas	mohammadi	REmam
	2009-10-12 17:16:45		office/word	no	no	3897.doc	doc	ara fas	REmam	
	2009-10-11 08:09:53		office/word	no	no	3897.doc	doc	ara		Computer
	2009-10-11 08:09:53		office/word	no	no	3897.doc	doc	ara		Computer2
	2009-10-12 00:33:52		office/word	no	no			ara fas	REmam	REmam
	2009-10-12 20:16:42		office/word	no	no	Baan.doc	doc	ara fas	mohammadi	mail
	2009-10-12 20:16:42		office/word	no	no	Baan.doc	doc	ara fas		mail
	2009-10-12 14:21:10		office/word	no	no	Table.doc	doc	ara	S-Gharavi	By PARHIZ
	2009-10-12 14:21:10		office/word	no	no	Table.doc	doc	ara	By PARHIZ ID RJE270	
	2009-10-12 16:15:04		office/word	no	no	Baan.doc	doc	ara fas	mohammadi	mail
	2009-10-12 16:15:04		office/word	no	no	Baan.doc	doc	ara fas		mail
	2009-10-12 12:46:35		office/word	no	no			ara fas	Mortazavi	Mortazavi
	2009-10-11 08:09:04		office/word	no	no			ara fas		

Page 1 of 111 (Max. 200 rows per page)

Displaying 1 - 30 of 111



Email Addrs/Phone Numbers/Login etc

XK Metaviewer: dasteen_20091013_ss Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.corp.nsa.gov:443/XKEYSCORE/

Most Visited Smart Bookmarks JSIgnite R1 Yehia URN Mapper XKS-Central DoncPage - X-KEYSCORE...

JSIgnite R1 SEARCHLIGHT User... DoncPage - X-KEYSC... XK Metaviewer... A4314 /dasteen... TLNSFORE... https://p.../710.html XK Results...

This system is audited for USGID 18 and Human Rights Act compliance
TOP SECRET//COMINT//NOFORN

XKEYSCORE WILDCARD [REDACTED] .out

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation Menu

- System
- XKEYSCORE
- Technologies in Domain
- User Activity
- VLAN
- With File Transfer
- Web Proxy
- WireShark
- Common
- Dictionary Hits
- File Transfer
- MultiSearch
- Network Management
- User Activity
- VoIP
- Wireless
- Workflow Central
- Request
- All Workflows
- All Pending Workflows
- My Workflows
- Results
- My Recent Results
- My Previous Results
- My Archived Results
- My Ongoing Results
- My Downloads
- All Downloads
- All Recent Results
- All Previous Results
- All Archived Results
- All Ongoing Results
- Statistics
- Signal Acquisition
- Link Summarization
- Tagging
- Local Tagging
- Path Extractor
- Tasking
- With Tasking
- My Account

Histogram: @Domain Histogram Grid

Clear Selection

Histogram of: @Domain (Click Bar to Filter)

@Domain	Count
ssp.gob.mx	452
pfp.local	158
bmi.msfoc...	3
businessmon...	3
imc-ms-daemon	3
mail.norinco.cn	3
zhenthuo@.com	3
inwind.it	1
steels-net.cn	1

Pivot: Casenotation

dasteen_20091013_ss

Help Actions Reports View FILTERS

Mail User Name	Deletetime	Highlights	@Domain	Subject	Chain
[REDACTED]	2009-10-10 05:15:10	CNE	mail.norinco.cn	2840 senior contacts in India for zhe	0kqe00g01mrdb@mail.norinco.cn&kate.etrut
[REDACTED]	2009-10-10 05:15:10	CNE	businessmonitor.co	2840 senior contacts in India for zhe	0kqe00g01mrdb@mail.norinco.cn&kate.etrut
[REDACTED]	2009-10-10 05:15:10	CNL	bmi.msfoc...	2840 senior contacts in India for zhe	0kqe00g01mrdb@mail.norinco.cn&kate.etrut
[REDACTED]	2009-10-10 05:15:10	CNE	zhenthuo@.com	2840 senior contacts in India for zhe	0kqe00g01mrdb@mail.norinco.cn&kate.etrut
[REDACTED]	2009-10-10 05:15:10	CNE	ime.me.daemon	2840 senior contacts in India for zhe	0kqe00g01mrdb@mail.norinco.cn&kate.etrut
[REDACTED]	2009-10-12 06:29:00		steels.net.cn	2010 ewtree rolex	3djuliette@steels.net.cn&bvlgari@inwind.it
[REDACTED]	2009-10-12 06:29:00		Inwind.it	2010 ewtree rolex	3djuliette@steels.net.cn&bvlgari@inwind.it
[REDACTED]	2009-10-11 08:36:53	CNE	ssp.gob.mx	101009 EII LA PAZ, BAJA CALIFORNI	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNC	pfp.local	101009 EII MEXICALI, BAJA CALIFOR	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNL	ssp.gob.mx	101009 EII MEXICALI, BAJA CALIFOR	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNF	ssp.gob.mx	101009 EII LA PAZ, BAJA CALIFORNI	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNL	ssp.gob.mx	101009 EII LA PAZ, BAJA CALIFORNI	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNF	ssp.gob.mx	101009 EII CIUDAD JUÁREZ, CHIHUAH	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNL	ssp.gob.mx	101009 EII CIUDAD JUÁREZ, CHIHUAH	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNF	pfp.local	101009 EII LA PAZ, BAJA CALIFORNI	dgjet.analisis@pfp.local&eduardo.argote@e
[REDACTED]	2009-10-11 08:36:53	CNC	ssp.gob.mx	101009 EII GAI TAHU, CHIHUAHUA, ST	dgjet.analisis@pfp.local&eduardo.argote@e

Displaying 1 - 11 of 11

This system is audited for USGID 18 and Human Rights Act compliance
TOP SECRET//COMINT//NOFORN

dasteen_073014000125540656_1

xks-central.corp.nsa.gov:8443

HTTP Activity (FOGGYBOTTOM)



XK Metaviewer: drvermi_0 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.corp.nsa.c... XKEYSCORE

Most Visited Smart Bookmarks JSONout: R1 Yeha URN Mapper XKS-Central DnsPage - X-KEYSC... JSonout: R1 SEARCHLIGHT Que... DnsPage - X-KEYSC... XK Metaviewer: ... TUNINGFORK https://j.../710.html XK Search: HTTP A...

This system is audited for USSID 10 and Human Rights Act compliance
TOP SECRET//COMINT//NOFORN

XKEYSCORE Welcome [REDACTED] Log Out

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation Menu

- MultiSearch
- IP Addresses
- Mac Address
- Username
- Classic A-M
- Alert
- BlackBerry
- CNE
- Call Logs
- Category DNI
- Cellular DNI
- Cisco Passwords
- DNS
- Document Metadata
- Document Tagging
- Email Addresses
- Extracted Files
- Full Log DNI
- HTTP Activity
- IKE Parser
- Logins and Passwords
- Microplugin Metadata
- Classic N-Z
- KEYLOGGER
- Network Logs
- PDF Metadata

drvermi_0

Help Actions Reports View FILTERS:

21:10:44	Datetime End	Highlights	HTTP Type	Host	URL Path	URL Args	Search Terms	Language
21:10:44	2009-10-14 20:29:00	CNE	post	login.facebook.com	/	login_attempt=1		
21:10:44	2009-10-14 20:29:00	CNE	get	www.facebook.com	/			
21:10:44	2009-10-14 20:29:00	CNE	get	www.14october.com	/	newsid=5fb5c038-f25		
21:10:44	2009-10-14 20:29:00	CNE	post	www.14october.com	/	partid=6f4c8fae-e1c2		
21:10:44	2009-10-14 20:29:00	CNE	get	ar-ar.facebook.com	/			
21:10:44	2009-10-14 20:29:00	CNE	get	forum.koocora.com	/	f=133		
21:10:44	2009-10-14 20:29:00	CNE	get	forum.koocora.com	/	f=133		
21:10:44	2009-10-14 20:29:00	CNE	get	forum.koocora.com	/	t=19827269		
21:10:44	2009-10-14 20:29:00	CNE	get	about				
21:10:44	2009-10-14 20:29:00	CNE	get	about				
21:10:44	2009-10-14 20:29:00	CNE	get	forum.koocora.com	/	t=19800405		
21:10:44	2009-10-14 20:29:00	CNE	get	static.ak.facebook.com	/common/	index=0		
21:10:44	2009-10-14 20:29:00	CNE	get	www.google.com.sa	/	hl=ar&source=hp&q=		
21:10:44	2009-10-14 20:29:00	CNE	post	login.facebook.com	/	login_attempt=1		
21:10:44	2009-10-14 20:29:00	CNE	post	login.facebook.com	/	login_attempt=1		
21:10:44	2009-10-14 20:29:00	CNE	get	www.google.com.sa	/	hl=ar&source=hp&q=		
21:10:44	2009-10-14 20:29:00	CNE	get	www.facebook.com	/friends/	ref=tn		
21:10:44	2009-10-14 20:29:00	CNE	get	www.google.com.sa	/	hl=ar&source=hp&q=		
21:10:44	2009-10-14 20:29:00	CNE	get	static.ak.facebook.com	/common/	index=0		
21:10:44	2009-10-14 20:29:00	CNE	get	www.26sep.net	/	lng=arabic&sid=5782		
21:10:44	2009-10-14 20:29:00	CNE	get	login.facebook.com	/	login_attempt=1		

HTTP Activity (FOGGYBOTTOM)



XK Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.corp.nsaic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session+Viewer&viewUri=%2FKEYSCORE%2FmetaViewer%2Fmetadata%2FviewSession.do%2F

This system is audited for USGID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA,AUS,CAN,GBR,NZL

X-KEYSCORE C2C Session Viewer

Session 7 of 6704 | Read-ahead: On

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2009-10-14 21:10:44	YM.VALAGWAAADTC						31515

Session Header (3) Meta (1)

Formatters: 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
 - :0 ->
 - :0
 - Find application
 - dnt_payload/browser

AUTO FORMATTER: app_id= dnt_payload/browser Viewer= DNT_PAYLOAD formatter: Info=

BROWSER INFO

Target Time: 2009-10-14T22:18:22
 Time Zone Offset: 3:00
 Local Time GMT: 2009-10-14T19:12:19+00:00

The URL visited was:

<http://www.altaurane.ws/news.aspx?title=♦♦♦♦♦&pageid=11>

The HTTP Post was:

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=dDw50DEzOTU20Dc7dDw7bDxpPDE%2B0z47bDxOPDtsPGk8t

This system is audited for USGID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA,AUS,CAN,GBR,NZL

Done

xks-central.corp.nsaic.gov:8443



CNE Specific Searches

CNE Search



XK Search: CNE - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/

Most Visited Smart Bookmarks DSignout: R1 Veeba URN Mapper KKS-Central DnsPage - XKEYSC...

DSignout: R1 SEARCH-LIGHT Que... DSignout - XKEYS... XK Search: CNE TUNINGFORK https://j.../710.html XK Search: HTTP A...

This system is audited for USSID 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL //20320108

XKEYSCORE Welcome Log Out

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation Menu

- MultiSearch
 - IP Addresses
 - Mac Address
 - Username
- Classic A-M
 - Alert
 - BlackBerry
 - CNE
 - Cell Logs
 - Category DNI
 - Cellular DNI
 - Cisco Passwords
 - DNS
 - Document Metadata
 - Document Tagging
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - HTTP Activity
 - IKE Parser
 - Logins and Passwords
 - Microplugin Metadata
- Classic N-Z
 - KEYLOGGER
 - Network Logs
 - PDF Metadata
 - PILEBEAM
 - PPF VoIP Metadata
 - Passport
 - Phone Number Extract
 - RBGAN
 - REGISTRY

Help

Fields Advanced Features Show Hidden Search Fields Clear Search Values Reload Last Search Values

Search: CNE

Query Name: [REDACTED]

Justification: [REDACTED] [Recent Justifications](#)

Additional Justification: [REDACTED]

Miranda Number: [REDACTED]

Datetime: 1 Day Start: 2009-10-14 00:00 Stop: 2009-10-15 23:59

Collection Technique: [REDACTED]

Username<realm>: [REDACTED]

IP Address: [REDACTED] From [\[IP Address Field Builder\]](#)

IP Address: [REDACTED] To [\[IP Address Field Builder\]](#)

Port: [REDACTED] From [\[Port Field Builder\]](#)

Port: [REDACTED] To [\[Port Field Builder\]](#)

Keylogger (search)

Scards KEYLOGGER Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://keys-me.mip.nsi.gov:9443/KEYSCORE/

Most Visited Email Backlinks Gigout R1 Yeha URN Mapper XKC-Central DnsPage - K-KEYSC...

Signature P.D. SEARCHLIGHT... DonePage XK... XK Metadata... XK Logon XKU (change...) TUNINGPORT XK Results Results 710.html XK Search...

This system is audited for USAGID 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL //20320109

KKEYSCORE Welcome [REDACTED] Log Out

Home Admin Users Search Workflow Center Results Reports Streams My Account XK Forum Help

Navigation Menu

- Call Manager
- Cellular DNS
- Cisco Passwords
- DNS
- Document Metadata
- Document Tagging
- Email Addresses
- Extracted Files
- Full Log DM
- HTTP Activity
- IFF Parser
- Logs and Passwords
- Microsoft Metadata
- Create N-Z
- KEYLOGGER
- Network Logs
- PDF Metadata
- PLISTBM
- PPTVdP Metadata
- Passport
- Phone Number Extractor
- PSOAN
- REGISTRY
- RTP
- Radio Logs
- RP
- SSL Parser
- Tech Strings in Document
- User Activity
- WLAN
- Web File Transfer
- Web Proxy
- Wireless
- Contact
- Dictionary Lists
- File Transfer
- MultiSearch
- IP Addresses
- Mac Addresses

Help

Feds Advanced Features Show Hidden Search Fields Clear Search Values Refresh List Search Values

Search: KEYLOGGER

Query Name: [REDACTED]

Justifications: [REDACTED] [Recent Justifications](#)

Additional Justification: [REDACTED]

Miranda Number: [REDACTED]

Datetimes: 1 Day Start: 2009-10-13 00:00 Stop: 2009-10-14 23:59

Collection Technique: [REDACTED]

Process Name: [REDACTED]

Window Name: [REDACTED]

Session ID: [REDACTED]

Process ID: [REDACTED]

Time: [REDACTED]

Key Strokes: [REDACTED]

Username<realm>: [REDACTED]

IP Address: [REDACTED] From [REDACTED] [IP Address Field Builder]

IP Address: [REDACTED] To [REDACTED] [IP Address Field Builder]

Keylogger (results)



XKEYSCORE Welcome: [REDACTED] Log Out

This system is audited for USGIC 18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Navigation Menu

- Caliper DNI
- Coco Passwords
- DNS
- Document Metadata
- Document Tagging
- Email Addresses
- Extracted File
- Full Log DNI
- HTTP Activity
- IE Parser
- Logins and Passwords
- Micropiggy Metadata
- Cloud N Z
- KEYLOGGER**
- Network Logs
- PDF Metadata
- PLBEAM
- PTT VoIP Metadata
- Pxeport
- Phone Number Extract
- R3CAN
- Roots Hy
- RTP
- Radmin Logs
- SP
- SSL Parser
- Tech Strings in Domains
- User Activity
- Wi-Fi
- Web File Transfer
- Web Proxy
- WireShark
- Common
- Dictionary Hits
- File Transfer
- MultiSearch
- IP Addresses

keylogger

Start Date	End Date	Host Source	Proc Name	Window Name	Session ID	Proc ID	Time	Key Strokes	Duration
2009-10-13	2009-10-13	GREENCHAOS15	QQ.exe	腾讯	3	804	2009-10-13 07:42:46	[ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl]	10ms
2009-10-13	2009-10-13	GREENCHAOS15	QQ.exe	腾讯	3	804	2009-10-13 07:42:46	刚刚和你谈去了吗?	10ms
2009-10-13	2009-10-13	GREENCHAOS15	QQ.exe	腾讯	3	804	2009-10-13 07:42:46	[0x10][ctrl][backspace]	10ms
2009-10-13	2009-10-13	GREENCHAOS15	QQ.exe	腾讯	3	804	2009-10-13 07:43:06	[0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0][0xe0]	10ms
2009-10-13	2009-10-13	GREENCHAOS15	QQ.exe	腾讯	3	804	2009-10-13 07:43:22	[backspace][ctrl]	10ms
2009-10-13	2009-10-13	GREENCHAOS15	QQ.exe	最近有点累	3	804	2009-10-13 07:44:02	[0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5][0xe5]	10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:13	3		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:13	[RunPad-3]24		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:16	3		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:16	[RunPad-3]42		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:46:30	2		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:20	[RunPad-2]53		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:24	6		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:24	[RunPad-6]26		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.FIF	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:35	9		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:35	[RunPad-9]03		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:43	3		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:43	[RunPad-3]28		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:51	[delete]7		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:54	[RunPad-7]		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:46:08	7		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:45:58	[RunPad-7]0		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:46:01	[RunPad-1]41		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:46:05	1		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:46:05	[RunPad-1]24		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:46:04	[delete]0		10ms
2009-10-13	2009-10-13	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C正书录入	552	2009-10-13 07:46:39	[RunPad-3]82		10ms

Keylogger (session via VNC)



The screenshot shows the XK Session Viewer interface in Mozilla Firefox. The title bar reads "XK Session Viewer - Mozilla Firefox". The address bar contains the URL "https://xk-cne.corp.usic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session%20Viewer&rowUrl=%2FKEYSCORE%2Fmetamover%2Fmetadata%2FviewSession.do%3Fid%3D93%26queryId%3Dmverni_002067900125552". A red banner at the top states "This system is audited for USSID 18 and Human Rights Act compliance" and "CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL". The main window title is "X-KEYSCORE [C2C Session Viewer [from archive]]". The table header includes columns for Datetime, Case Notation, From IP, To IP, From Port, To Port, Protocol, and Length. A row shows "2009-10-13 16:13:43" and "CC.RMSXXXXAHZDT0" with a length of "31186". Below the table are tabs for "Session", "header (3)", and "Meta (1)". The "Session" tab is selected. The "Formatter" dropdown is set to "AUTO". The "KEYLOGGER" section displays a table of keystroke logs. The table has columns for Window Title, Process Name, and Application Name. Rows show entries for QQ.exe, EXCEL.EXE, and MSACCESS.EXE processes. The "One-Click Search" sidebar is visible on the left.

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2009-10-13 16:13:43	CC.RMSXXXXAHZDT0						31186

Session header (3) Meta (1)

Formatter: AUTO | Send to: Download Session | Mode: Snippet | Options | search content: Enter text to search | clear | ▲

KEYLOGGER

Output columns are designated by process name/process id/session id

Keystroke Legend

	QQ.exe/8040	EXCEL.EXE/552/0	MSACCESS.EXE/1580/0	MSACCESS.EXE/1580/0
Window Title:	猝想	Microsoft Excel - 3C证书导入工作 周报0928-1001.xls	Microsoft Access	Microsoft Access
2009-10-13T07:42:45.406	[ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl]			
2009-10-13T07:42:46.781	那标准和非标进去了吗？			
2009-10-13T07:42:46.796	[0x16][ctrl][>s]			
2009-10-13T07:43:6.921	[0xe5]B[0xe5][0xe5][0xe5]AO[0xe5] [0xe5]ZHI[0xe5]U[0xe5]N[0xe5] [0xe5]HE[0xe5][0xe5] [0xe5]F3[0xe5][0xe5]E[0xe5][0xe5] [0xc5]AO[0xc5][0xc5]L[0xc5]0[0xc5] [0xe5]ZJO[0xe5][0xe5]JI[0xe5] [0xe5]AN[0xe5][0xe5][0xe5]DE[0xe5] [0xe5]0[0xe5]2[0xe5][0xe5]YE[0xe5] [0xe5]JBU[0xe5][0xe5][0xe5]ZHI[0xe5] [0xc5]D[0xc5]AO[0xc5][0xc5] [0xe5]JI[0xe5]N[0xe5][0xe5]QU[0xe5] [0xe5]ME[0xe5][0xe5][0xe5]NE[0xe5] [sd][0xe5][s1][~]			
2009-10-13T07:43:22.15	[bs][ctrl]			
Window Title Changed:	最近有点烦			
	[0xe5]B[0xe5]U[0xe5][0xe5]			

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

Expanded!

The logo for KeyScore, featuring the word "KEYSCORE" in a blue, stylized font with a white outline, set against a background of three large, metallic-looking pyramids.

Registry

The screenshot shows a Mozilla Firefox browser window with the title "XK Metaviewer: UserAssistKey (WORKFLOW) - Mozilla Firefox". The address bar displays the URL <https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/>. The page content is a "UserAssistKey (WORKFLOW)" view. At the top, it says "This system is audited for USSID 18 and Human Rights Act compliance" and "TOP SECRET//COMINT//REL TO USA, CAN, GBR". Below this, there's a navigation menu with links like Home, Admin, Users, Search, Workflow Central, Results, Statistics, Tagging, Tasking, My Account, XK Forum, and Help.

The main area has tabs for "Help", "Actions", "Reports", "View", and "FILTERS". A table titled "Hive" lists registry keys under "HKEY_USERS". The table includes columns for Hive, Key, Value, Type, Num S, Num V, and Modif. The data shows three entries:

Hive	Key	Value	Type	Num S	Num V	Modif
HKEY_USERS	S-1-5-21-1060264298-920026266-1202660629-1003\Software\Microsoft\Windows\CurrentVersion\Run\{d5f562e0-3c57-20ec-0000-000000000000}	{d5f562e0-3c57-20ec-0000-000000000000}	Key	0	29	2010-10-12 12:38:13
HKEY_USERS	S-1-5-21-2362634650-3895404499-1650422205-4532\Software\Microsoft\Windows\CurrentVersion\Run\{d5f562e0-3c57-20ec-0000-000000000000}	{d5f562e0-3c57-20ec-0000-000000000000}	REG_BINARY	0	0	2010-10-12 12:38:13
HKEY_USERS	S-1-5-21-2362634650-3895404499-1650422205-4532\Software\Microsoft\Windows\CurrentVersion\Run\{d5f562e0-3c57-20ec-0000-000000000000}	{d5f562e0-3c57-20ec-0000-000000000000}	Key	0	1	2010-10-12 12:38:13

Below the table is a "XK Session Viewer - Mozilla Firefox" window. It shows a session list with one entry: "Session 1 of 91" from IP "10.10.10.10" on port "80" to "10.10.10.10" on port "80". The session details show "Datetime: 2009-10-12 12:38:13" and "Case Notation: AJ.STZAAJMAADTC". The "REGISTRY QUERY" section at the bottom shows a tree structure of registry keys under "HKEY_USERS\S-1-5-21-2362634650-3895404499-1650422205-4532\Software\Microsoft\Windows\CurrentVersion\Run".



wrap Up



Payloads Handled

Parsing

- Browser Info
- Collected Files
- Directory Walks
- Drive Listings
- Ipconfig
- Keylogger
- Process Lists
- Registry
- System Survey (partial)

Tailored Viewing

- yes
- standard XKS view
- yes
- xml
- xml
- yes
- xml
- yes
- xml



Other Payloads

- arpcache
- arpconfiguration
- auditinformation
- capturedcredentialsdata
- connectionlog (unavailable)
- datatransmission
- email
- error
- exchangedata
- fb
- filefilterlist
- localeinformation
- modulelist
- machineinformation
- netmap
- networkmapping
- netstat
- networkstatistics
- systime
- routing
- routingconfiguration
- sleepysheriff
- smackcrafty
- storedfile
- systemsurvey
- systemversion
- transportlist
- unidentifiedfile
- wirelesssurvey



Tech Strings in Documents

- Catchall for data types without plugins

XK Metaviewer: vpn in docs - Mozilla Firefox

File Edit View History Bookmarks Tools Help

<https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/>

Most Visited Smart Bookmarks DSignout: RL Yehia URN Mapper XKS-Central DnsPage - XKEYSC... DSignout: RL SEARCHLIGHT Quer... DnsPage - XKEYS... XK Metaview... #4314 (change the ... TUNINGFORK https://o.../210.html XK Results

This system is audited for USSIPO 18 and Human Rights Act compliance
TOP SECRET//COMINT//NOFORN

XKEYSCORE Welcome Log Out

Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help

Navigation Menu

- SSL Parser
- Tech Strings in Docs
- User Activity
- VLAN
- Web File Transfer
- Web Proxy
- Wireshark
- Common
- Dictionary Hits
- File Transfer
- MultiSearch
- Network Management
- UserActivity
- VoIP
- Wireless
- Workflow Central
- Request
- All Workflows
- All Pending Workflows
- My Workflows
- Results
- My Recent Results
- My Previous Results
- My Archived Results
- My Ongoing Results

vpn in docs

Help Actions Reports View FILTERS:

Highlights	ID	Datetime	Datetime End	Event Type	Tech Dictionary	Tech Nk	Tech Value	Tech Filename	Application
	67	2009-10-13 11:27:33	2009-10-13 11:27:35	email_body	classic	vpn	vpn		mail/webmail/vbulletin
	68	2009-10-13 11:28:04	2009-10-13 11:28:11	email_body	classic	vpn	vpn		mail/webmail/vbulletin
OE	154	2009-10-12 06:38:26	2009-10-12 06:00:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	155	2009-10-12 06:38:30	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	156	2009-10-12 06:38:33	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	157	2009-10-12 06:38:42	2009-10-12 06:01:00	tech_body	classic	vpn	pptp		dnt_payload/dnt_payload
OE	158	2009-10-12 06:38:42	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	159	2009-10-12 06:38:43	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	160	2009-10-12 06:38:47	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	161	2009-10-12 06:38:48	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	162	2009-10-12 06:38:54	2009-10-12 06:10:00	tech_body	classic	vpn	pptp		dnt_payload/dnt_payload
OE	163	2009-10-12 06:38:54	2009-10-12 06:10:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	164	2009-10-12 06:38:56	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	174	2009-10-12 09:25:25	2009-10-12 09:13:00	document_body	classic	vpn	vpn	H:\THI-095CC.DOC	dnt_payload/file
OE	218	2009-10-12 11:37:21	2009-10-12 11:27:00	document_body	classic	vpn	vpn	H:\new Folder (3)\img	dnt_payload/file
OE	219	2009-10-12 06:44:09	2009-10-12 06:10:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	220	2009-10-12 09:39:45	2009-10-12 09:26:00	email_body	classic	vpn	vpn		dnt_payload/file
OE	225	2009-10-13 06:37:34	2009-10-13 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	226	2009-10-13 06:37:43	2009-10-13 06:02:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload
OE	227	2009-10-13 06:37:59	2009-10-13 06:02:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_payload



Future Plans

- Expanded data coverage
 - UK, AUS, (NZL possibly)
 - Validator/FOX contact/survey flows??
 - ECI data??
 - Better TUCKER processing (both in TAO and XKS)
- Extended plug in coverage
 - Network information (neighbor/gateway IPs etc)
 - Machine Information (host name etc)
- Process files not found in passive
 - Registry files
 - Thumbs.db
 - Browser history/bookmarks
- Apply to Media Exploitation



Questions?

10 01 101 1001 1001 1001
1001 1 001 1001 11010101 101 101 101
1001 1001 1001 1001 1001 1001 1001 1001
0 10 01 101 1001 1001 1001 1001 1001
0 10 101 01 1001 1001 1001 1001 1001
0 01 10 101 1001 1001 1001 1001 1001
0 101 101 1001 1001 1001 1001 1001
0 01 10 101 1001 1001 1001 1001 1001

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



Blank

NEW!!

- Page

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