CNE Analysis in XKEYSCORE

15 October 2009

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

DERIVED FROM: NSA/CSSM 1-52
DATED: 20070108
DECLASSIFY ON: 20320108

XKEYSCORE

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

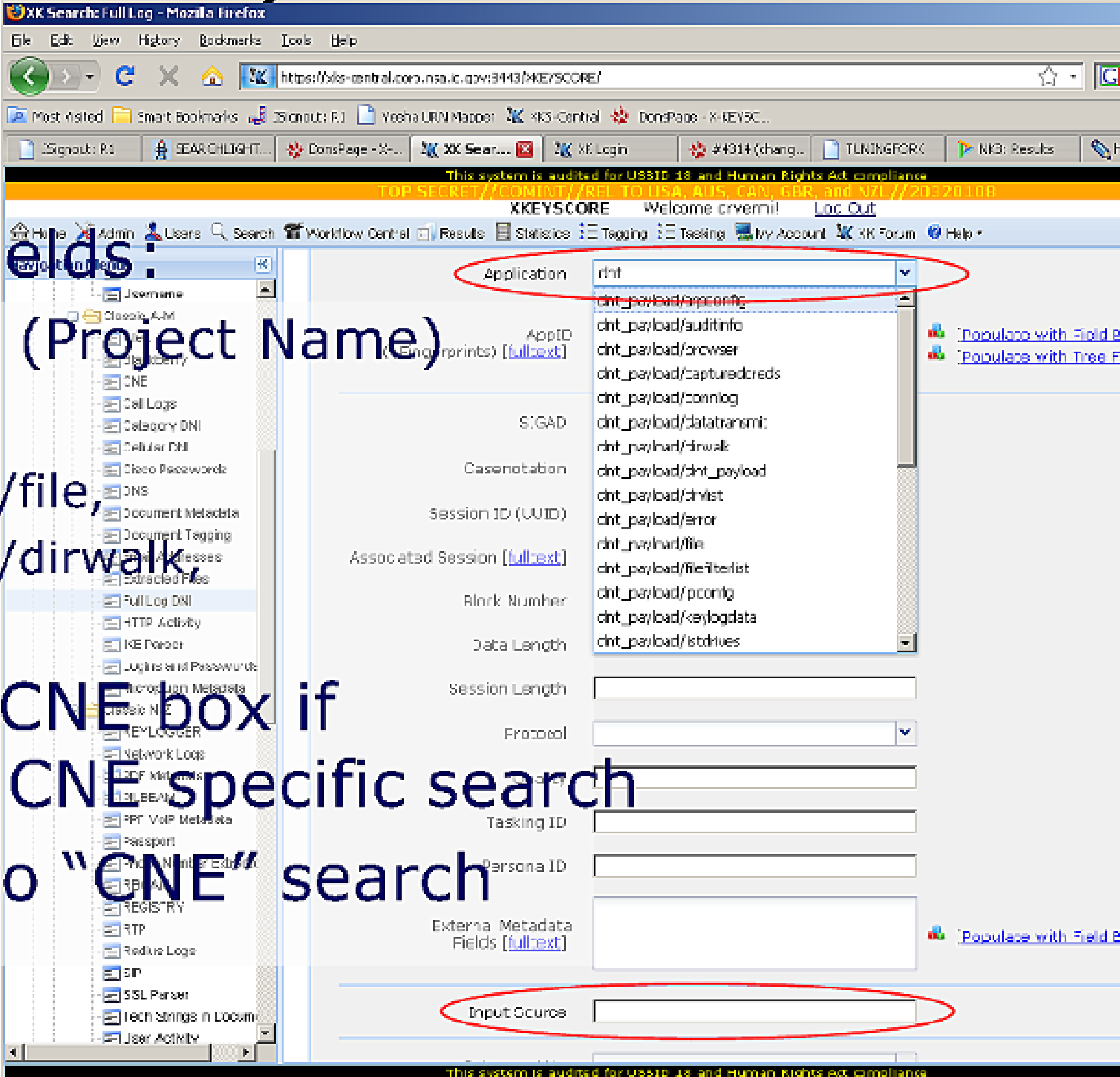
A “typical” day’s CNE results

```
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

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

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 cryerml! Log Out

Application: dnt

- dnt_payload/appconfig
- dnt_payload/auditinfo
- dnt_payload/browser
- dnt_payload/capturedcreds
- dnt_payload/connlog
- dnt_payload/datatransmit
- dnt_payload/dirwalk
- dnt_payload/dnt_payload
- dnt_payload/dnlist
- dnt_payload/error
- dnt_payload/file
- dnt_payload/filefilterlist
- dnt_payload/pconfig
- dnt_payload/keylogdata
- dnt_payload/istdrives

AppID (Fingerprints) [fulltext]

SIGAD

Casenotation

Session ID (UUID)

Associated Session [fulltext]

Block Number

Data Length

Session Length

Protocol

Tasking ID

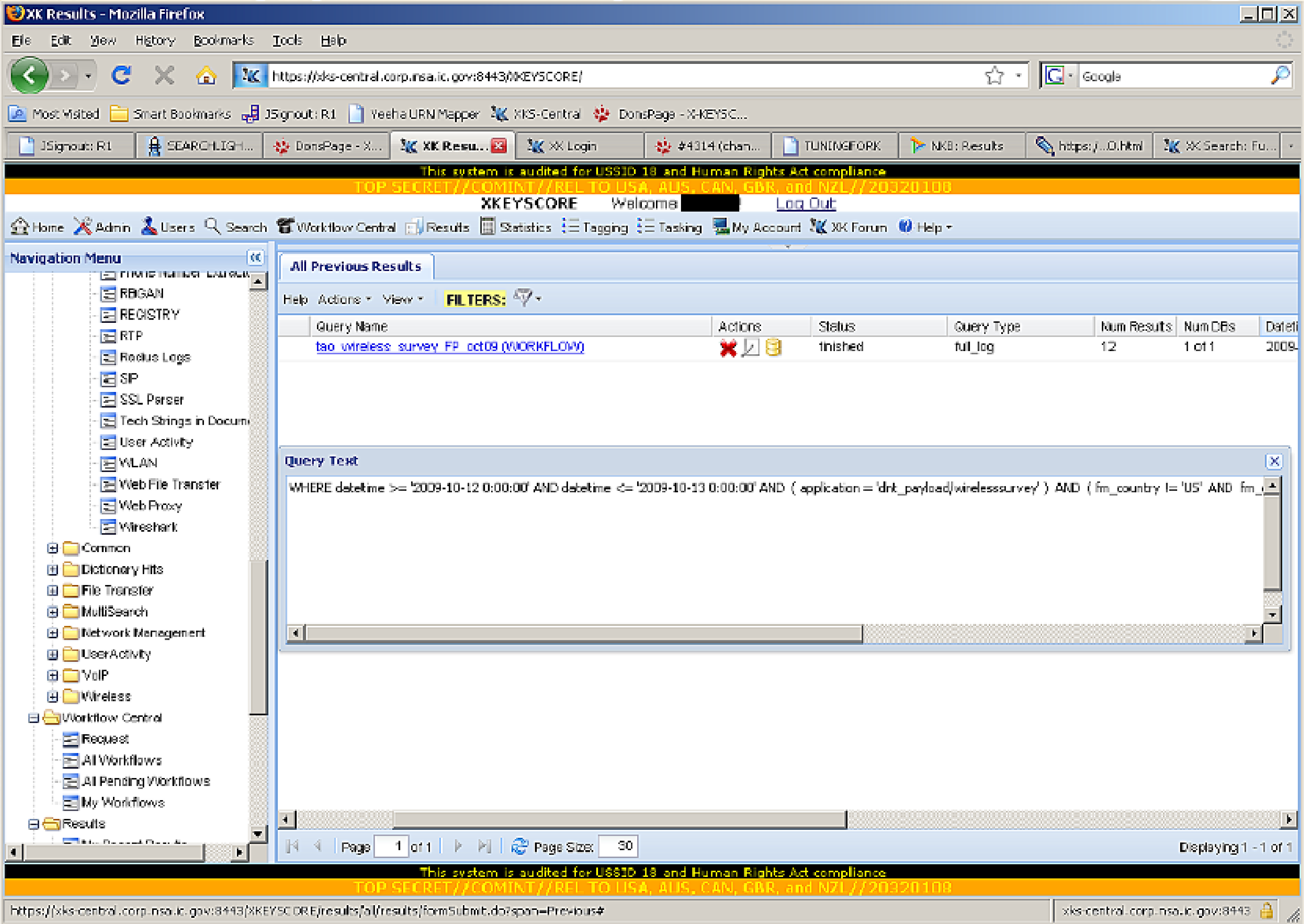
Persona ID

External Metadata Fields [fulltext]

Input Source

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

Full Log (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 [redacted] Log Out

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

Query Text

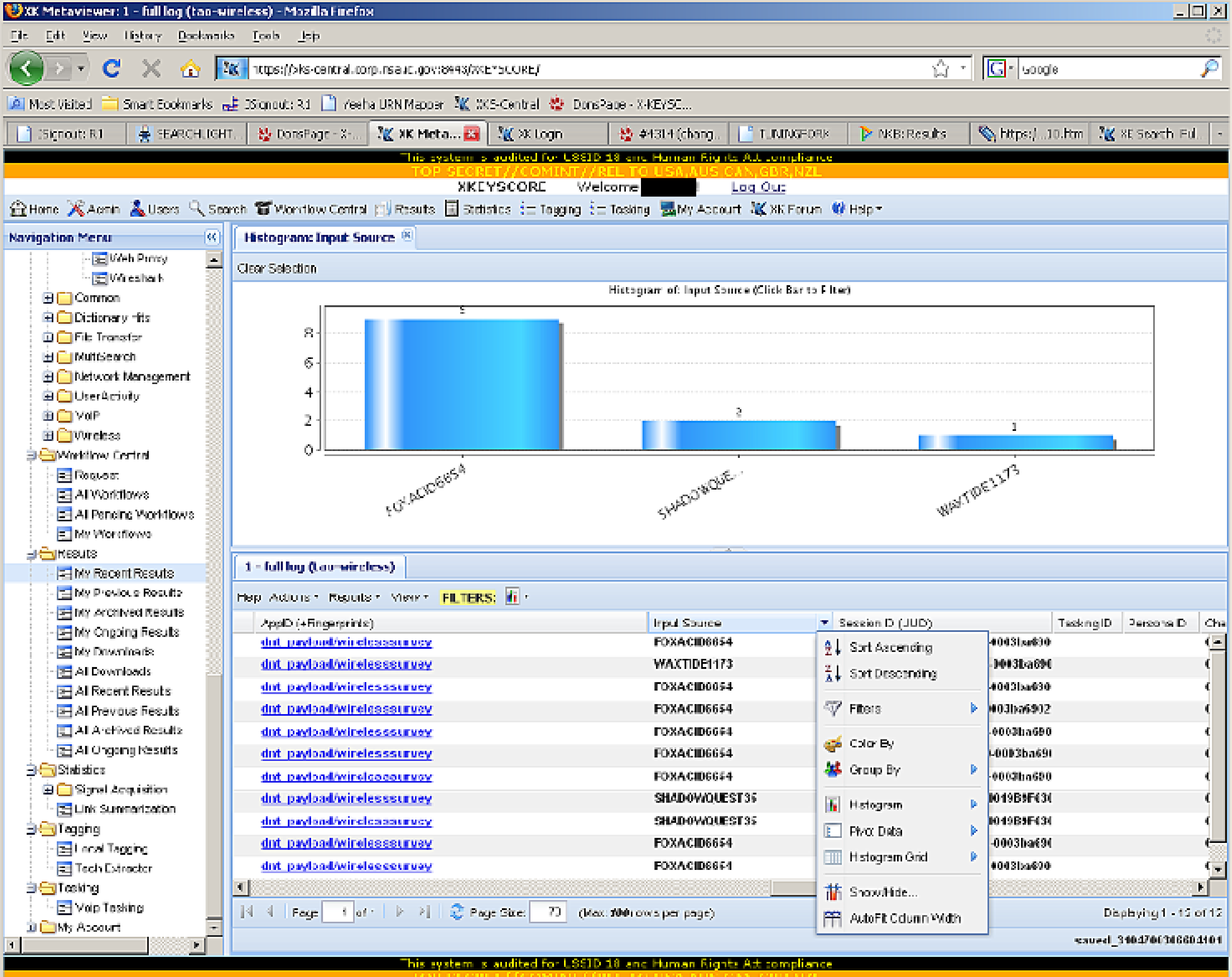
```
WHERE datetime >= '2009-10-12 0:00:00' AND datetime <= '2009-10-13 0:00:00' AND ( application = 'dnt_payload/wirelesssurvey' ) AND ( fm_country != 'US' AND fm_
```

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/all/results/formSubmit.do?span=Previous#

Results Manipulation



XK Metaviewer: 1 - full log (tao-wireless) - Mozilla Firefox

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

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

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

XKEYSCORE Welcome [redacted] Log Out

Histogram: Input Source

Clear Selection

Histogram of: Input Source (Click Bar to Filter)

1 - full log (tao-wireless)

	AppID (+Fingerprints)	Input Source	Session ID (UUID)	Tasking ID	Persona ID	Cha
	dnt_payload/wirelesssurvey	FOXACID6654	0003ba690			
	dnt_payload/wirelesssurvey	WAXTIDE1173	0003ba690			
	dnt_payload/wirelesssurvey	FOXACID6654	0003ba690			
	dnt_payload/wirelesssurvey	FOXACID6654	003ba6902			
	dnt_payload/wirelesssurvey	FOXACID6654	-0003ba690			
	dnt_payload/wirelesssurvey	FOXACID6654	-0003ba69			
	dnt_payload/wirelesssurvey	FOXACID6654	-0003ba690			
	dnt_payload/wirelesssurvey	SHADOWQUEST35	049B9F63			
	dnt_payload/wirelesssurvey	SHADOWQUEST35	049B9F63			
	dnt_payload/wirelesssurvey	FOXACID6654	-0003ba69			
	dnt_payload/wirelesssurvey	FOXACID6654	0003ba690			

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

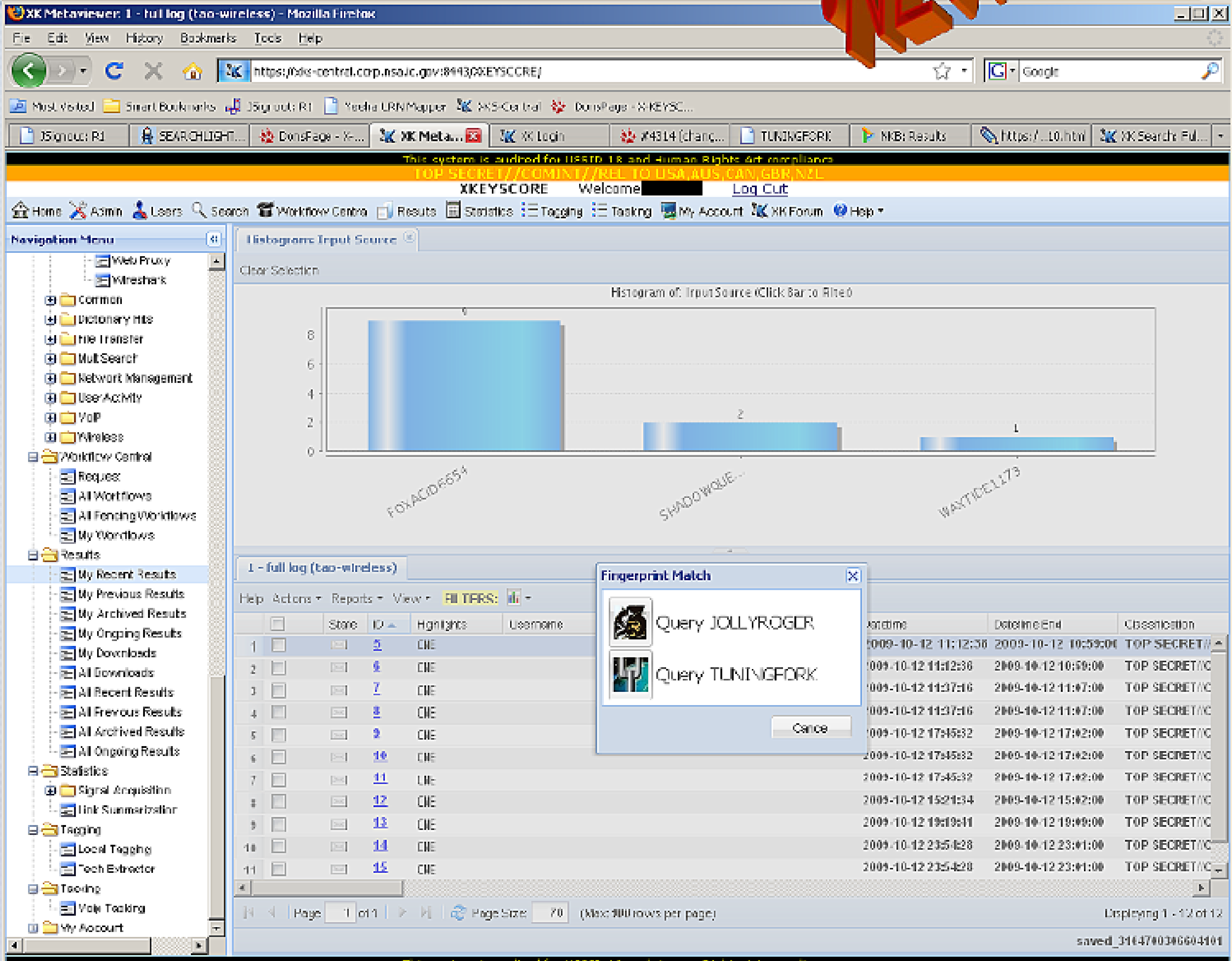
saved_340470034660404

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

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

Click Thru

NEW!!



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

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

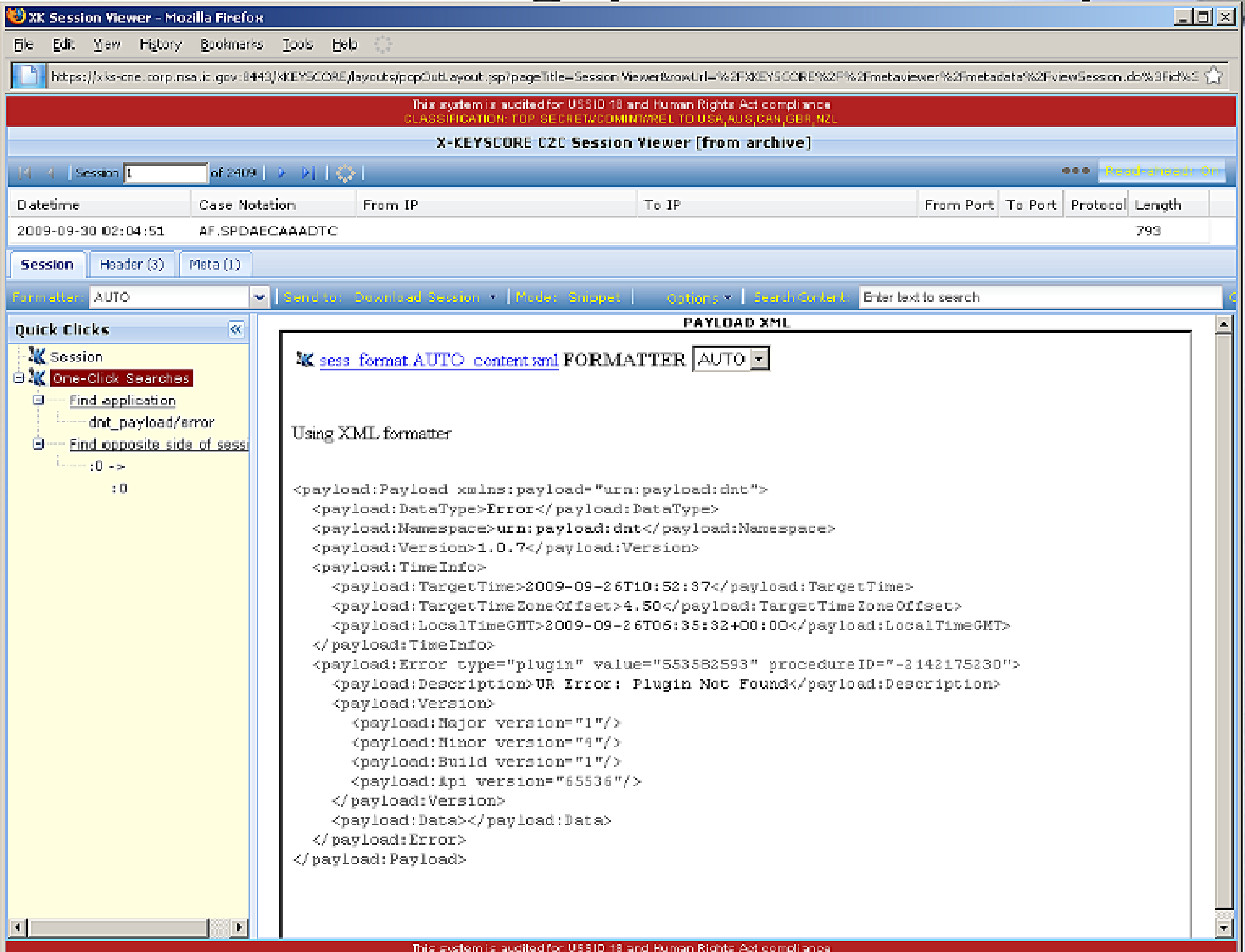
XKEYSCORE Welcome [redacted] Log Out

	☐	Store	ID	Highlights	Username	...atetime	Datetime End	Classification
1	☐	✉	5	CIE		2009-10-12 11:12:36	2009-10-12 10:59:00	TOP SECRET//
2	☐	✉	6	CIE		2009-10-12 11:12:36	2009-10-12 10:59:00	TOP SECRET//C
3	☐	✉	7	CIE		2009-10-12 11:37:16	2009-10-12 11:07:00	TOP SECRET//C
4	☐	✉	8	CIE		2009-10-12 11:37:16	2009-10-12 11:07:00	TOP SECRET//C
5	☐	✉	9	CIE		2009-10-12 17:45:32	2009-10-12 17:02:00	TOP SECRET//C
6	☐	✉	10	CIE		2009-10-12 17:45:32	2009-10-12 17:02:00	TOP SECRET//C
7	☐	✉	11	CIE		2009-10-12 17:45:32	2009-10-12 17:02:00	TOP SECRET//C
8	☐	✉	12	CIE		2009-10-12 15:21:34	2009-10-12 15:02:00	TOP SECRET//C
9	☐	✉	13	CIE		2009-10-12 19:19:11	2009-10-12 19:09:00	TOP SECRET//C
10	☐	✉	14	CIE		2009-10-12 23:54:28	2009-10-12 23:01:00	TOP SECRET//C
11	☐	✉	15	CIE		2009-10-12 23:54:28	2009-10-12 23:01:00	TOP SECRET//C

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

saved_3144700306604101

Session Viewing (XML Default)



https://xks-cne.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaviewer%2Fmetadata%2FviewSession.do%3Fid%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 C2C Session Viewer [from archive]

Session 1 of 2409

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

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

PAYLOAD XML

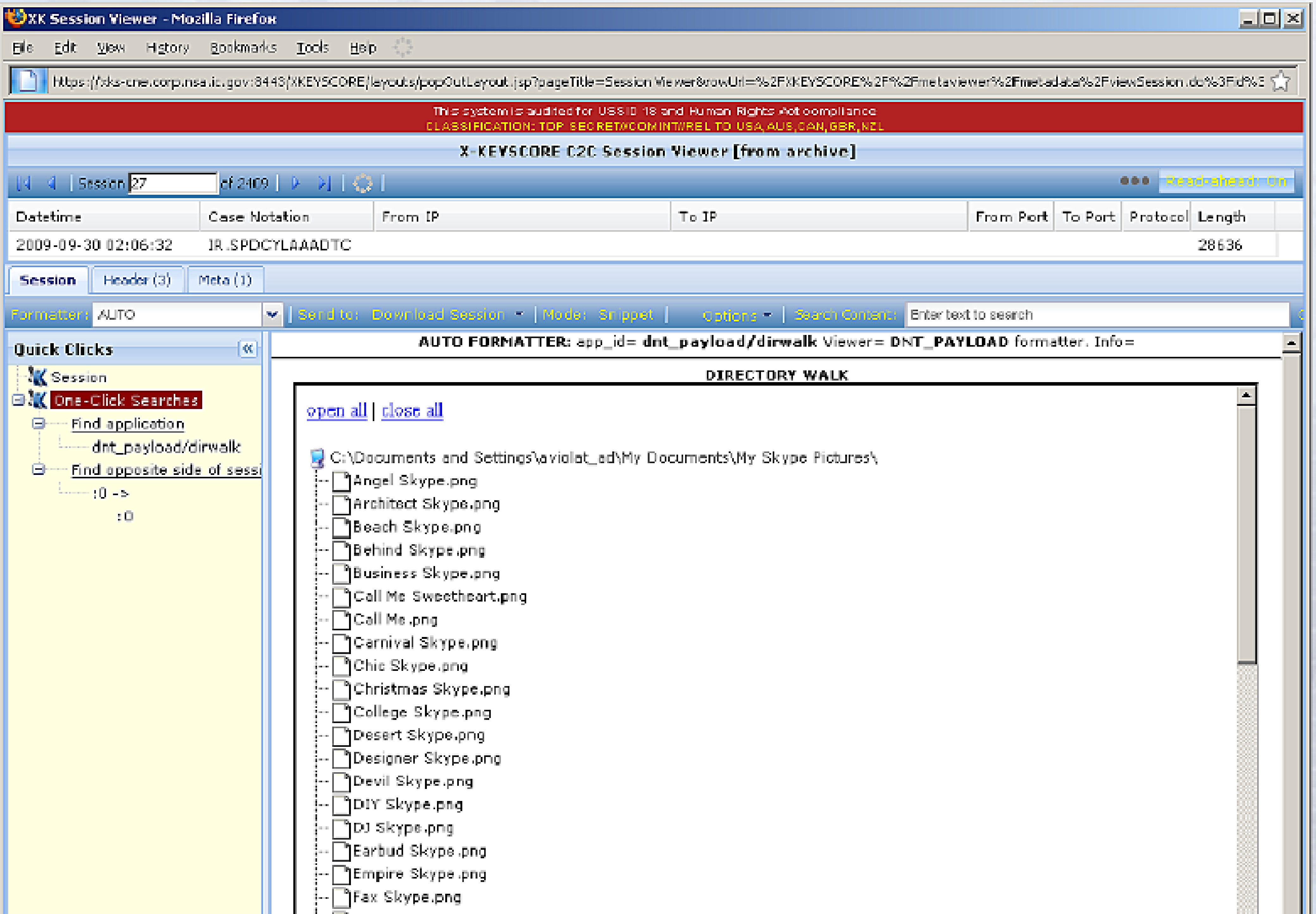
sess_format AUTO_content xml FORMATTER AUTO

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="553582593" 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>
```

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

Session Viewing (Specialized per payload)



XK Session Viewer - Mozilla Firefox
File Edit View History Bookmarks Tools Help

https://xks-cne.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaviewer%2Fmetadata%2FviewSession.do%3Fid%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 C2C Session Viewer [from archive]

Session 27 of 2409

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

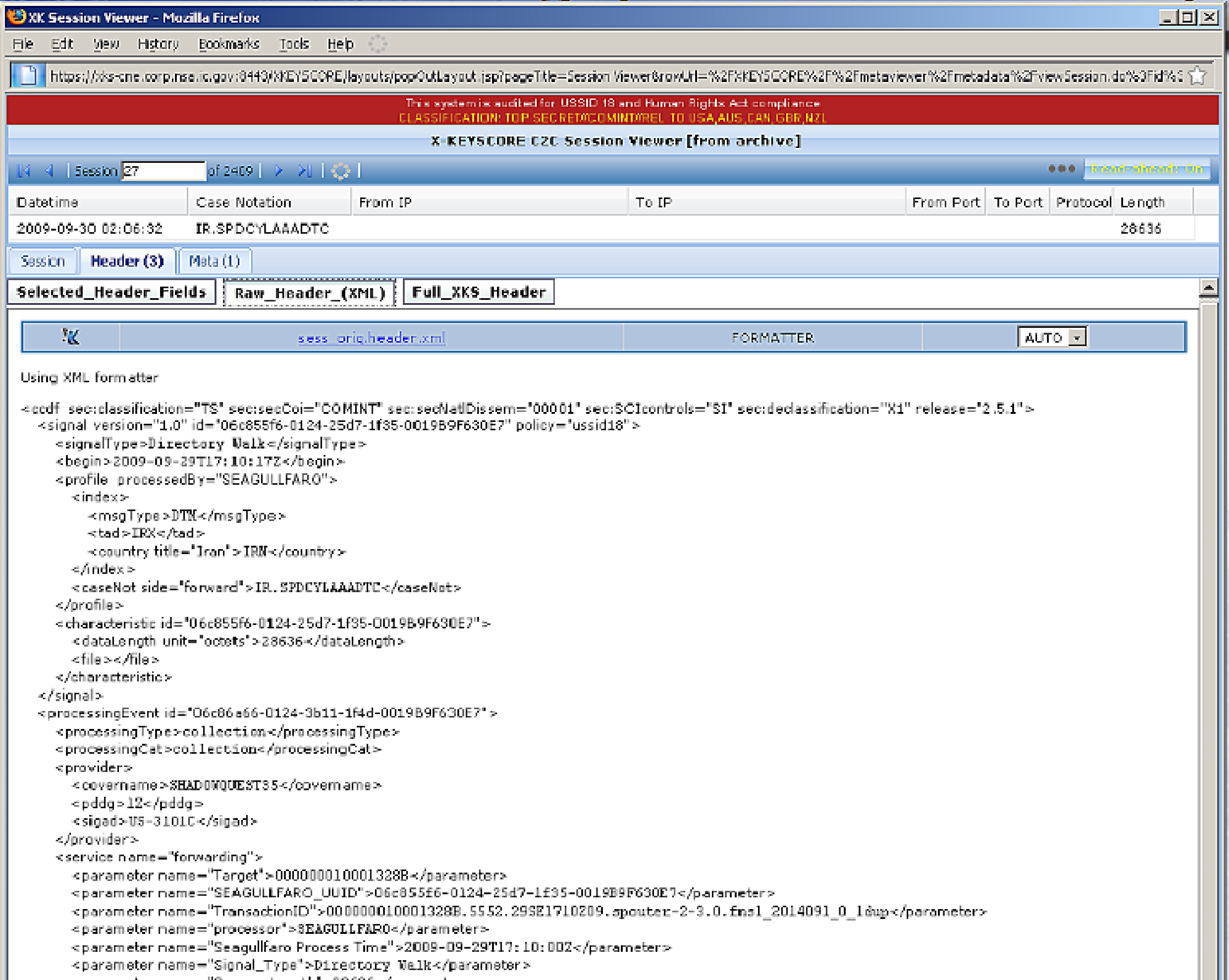
Formatter: AUTO | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

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

DIRECTORY WALK

```
C:\Documents and Settings\aviolat_ad\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)


XK Session Viewer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://xks-cne.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaviewer%2Fmetadata%2FviewSession.do%3Fid%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 C2C Session Viewer [from archive]
Session 27 of 2409
Read-ahead: On
Session
Header (3)
Meta (1)
Selected_Header_Fields
Raw_Header_(XML)
Full_XKS_Header
sess_orig.header.xml
FORMATTER
AUTO

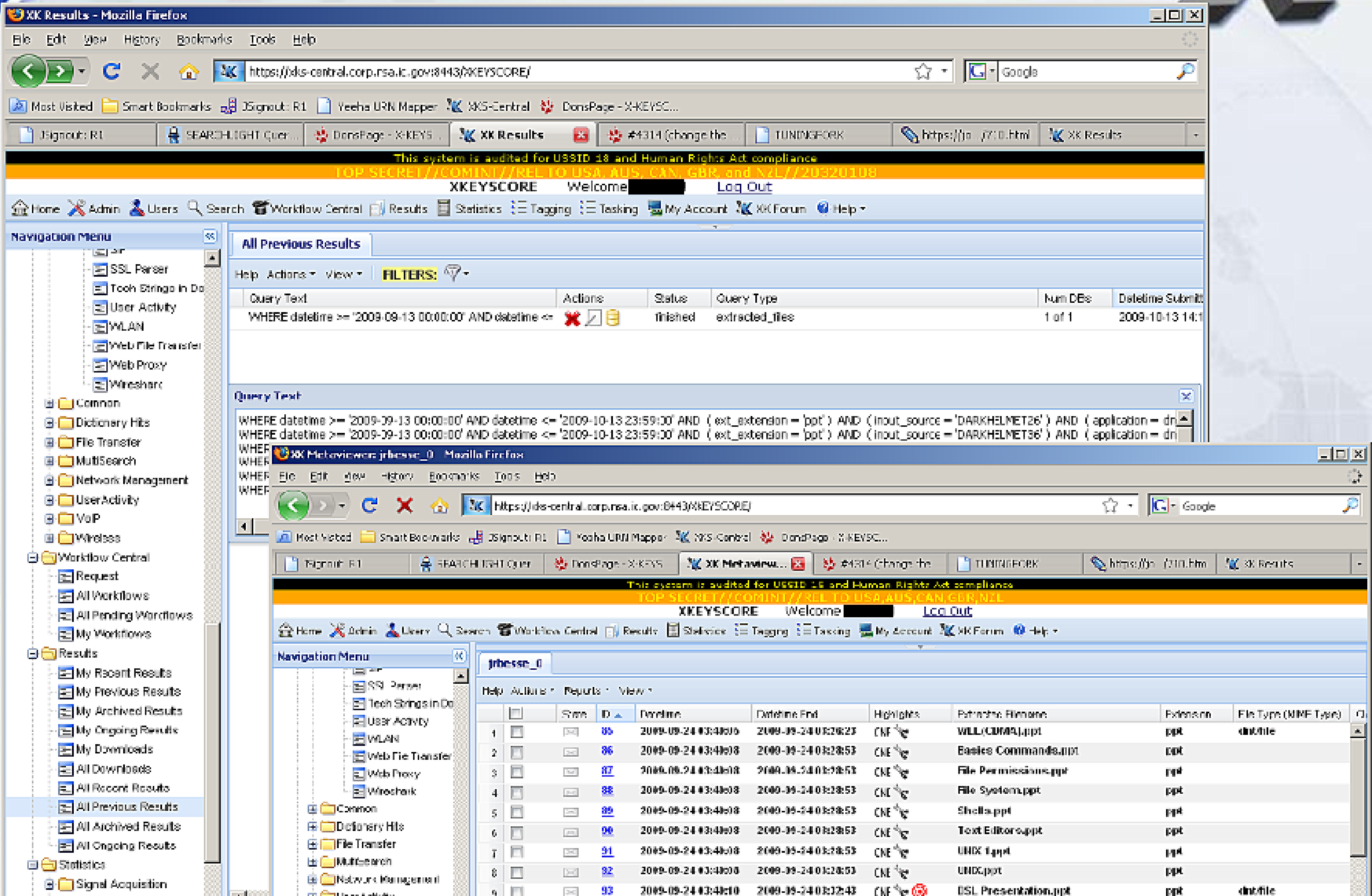
Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2009-09-30 02:06:32	IR.SPDCYLAAADTC						28636

Using XML formatter

```
<ccdf sec:classification="TS" sec:secCoi="COMINT" sec:secNatlDissem="00001" sec:SCIcontrols="SI" sec:declassification="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>DTM</msgType>
        <tad>IRX</tad>
        <country title="Iran">IRN</country>
      </index>
      <caseNot side="forward">IR.SPDCYLAAADTC</caseNot>
    </profile>
    <characteristic id="06c855f6-0124-25d7-1f35-0019B9F630E7">
      <dataLength unit="octets">28636</dataLength>
      <file></file>
    </characteristic>
  </signal>
  <processingEvent id="06c86a66-0124-3b11-1f4d-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.fms1_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>
```

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

Extracted Files–CNE Specific


XK Results - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/
Most Visited Smart Bookmarks JSignout: R1 Yeeha URN Mapper XKS-Central DonsPage - X-KEYSC...
JSignout: R1 SEARCHLIGHT Quer... DonsPage - X-KEYS... XK Results #4314 (change the... TUNINGFORK https://js.../7/0.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 [redacted] 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
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
All Previous Results
Help Actions View FILTERS:

Query Text	Actions	Status	Query Type	Num DBs	Datetime Submit
WHERE datetime >= '2009-09-13 00:00:00' AND datetime <=	✖	finished	extracted_files	1 of 1	2009-10-13 14:1

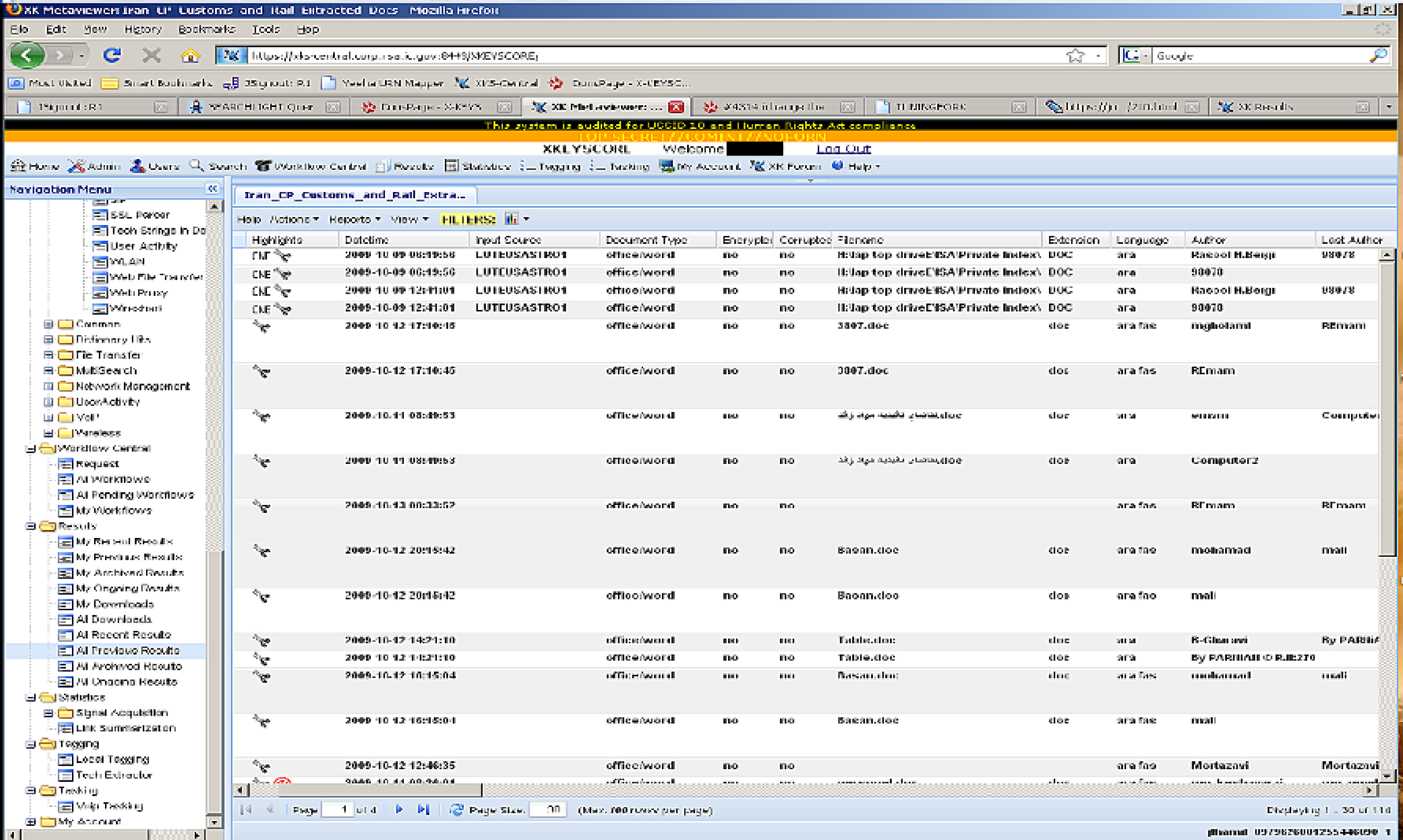
Query Text

```
WHERE datetime >= '2009-09-13 00:00:00' AND datetime <= '2009-10-13 23:59:00' AND ( ext_extension = 'ppt' ) AND ( input_source = 'DARKHELMET26' ) AND ( application = dn
WHERE datetime >= '2009-09-13 00:00:00' AND datetime <= '2009-10-13 23:59:00' AND ( ext_extension = 'ppt' ) AND ( input_source = 'DARKHELMET36' ) AND ( application = dn
WHER
WHER
WHER
WHER
```

XK Metaviewer: jrbesse_0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/
Most Visited Smart Bookmarks JSignout: R1 Yeeha URN Mapper XKS-Central DonsPage - X-KEYSC...
JSignout: R1 SEARCHLIGHT Quer... DonsPage - X-KEYS... XK Metaview... #4314 (change the... TUNINGFORK https://js.../7/0.htm 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 [redacted] 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
jrbesse_0
Help Actions Reports View

	□	State	ID	Datetime	Datetime End	Highlights	Extracted Filename	Extension	File Type (MIME Type)
1	□	✉	85	2009-09-24 03:40:06	2009-09-24 08:26:23	CNE	WLL(CDMA).ppt	ppt	dnt/file
2	□	✉	86	2009-09-24 03:40:08	2009-09-24 08:28:53	CNE	Basics Commands.ppt	ppt	
3	□	✉	87	2009-09-24 03:40:08	2009-09-24 08:28:53	CNE	File Permissions.ppt	ppt	
4	□	✉	88	2009-09-24 03:40:08	2009-09-24 08:28:53	CNE	File System.ppt	ppt	
5	□	✉	89	2009-09-24 03:40:08	2009-09-24 08:28:53	CNE	Shells.ppt	ppt	
6	□	✉	90	2009-09-24 03:40:08	2009-09-24 08:28:53	CNE	Text Editors.ppt	ppt	
7	□	✉	91	2009-09-24 03:40:08	2009-09-24 08:28:53	CNE	UNIX 1.ppt	ppt	
8	□	✉	92	2009-09-24 03:40:08	2009-09-24 08:28:53	CNE	UNIX.ppt	ppt	
9	□	✉	93	2009-09-24 03:40:10	2009-09-24 08:32:43	CNE	DSL Presentation.ppt	ppt	dnt/file

Document Metadata – Active/Passive Converged Analysis



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

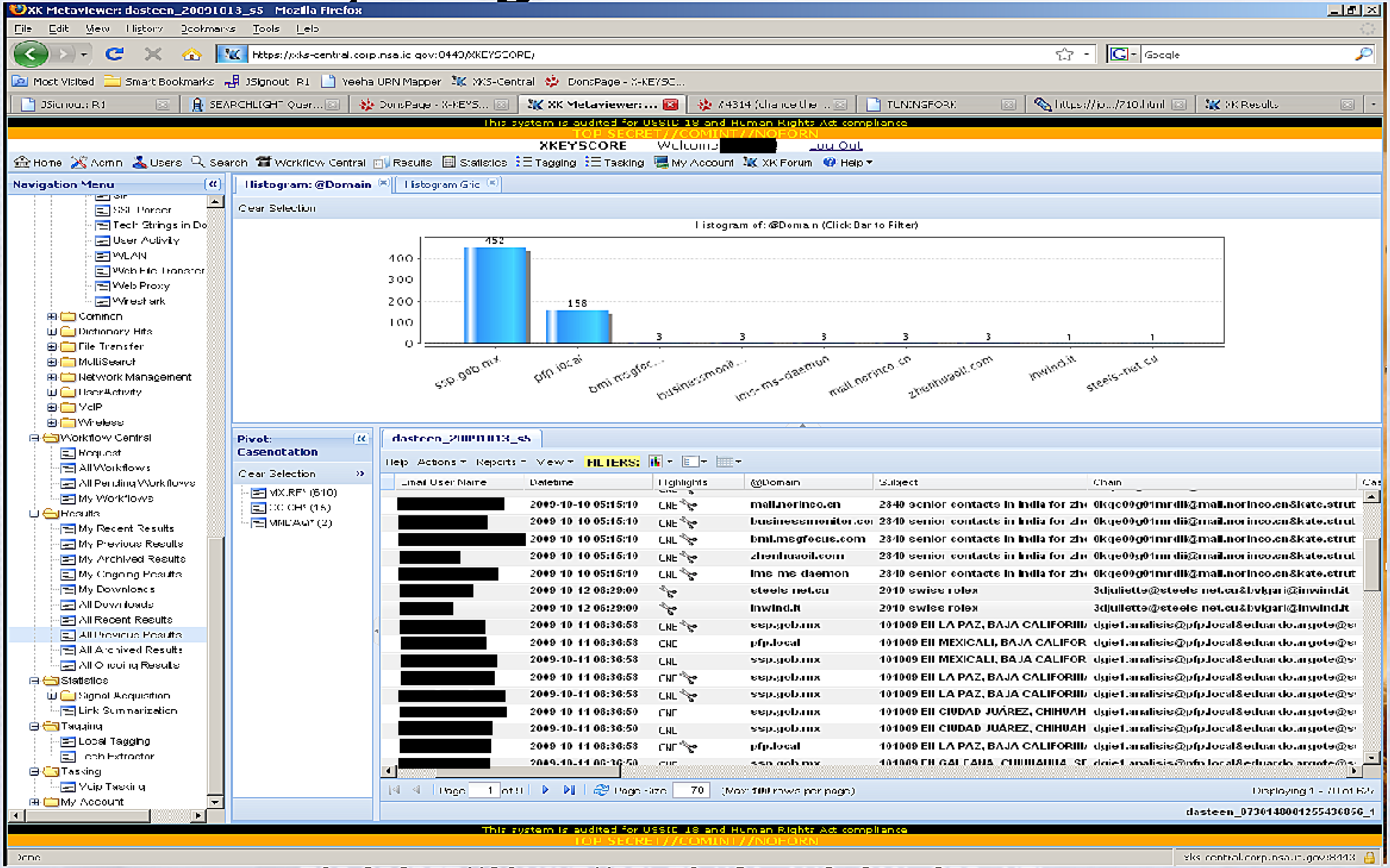
TOP SECRET//COMINT//NOFORN

XKEYSCORE Welcome [redacted] Log Out

Highlights	Datetime	Input Source	Document Type	Encrypted	Corrupted	Filename	Extension	Language	Author	Last Author
CNE	2009-10-09 08:49:58	LUTEUSASTR01	office/word	no	no	H:\lap top driveE\ISA\Private Index\	DOC	ara	Rasool H.Beigi	99078
CNE	2009-10-09 08:49:58	LUTEUSASTR01	office/word	no	no	H:\lap top driveD\ISA\Private Index\	DOC	ara	99078	
CNE	2009-10-09 12:41:01	LUTEUSASTR01	office/word	no	no	H:\lap top driveE\ISA\Private Index\	DOC	ara	Rasool H.Beigi	99078
CNE	2009-10-09 12:41:01	LUTEUSASTR01	office/word	no	no	H:\lap top driveD\ISA\Private Index\	DOC	ara	99078	
	2009-10-12 17:10:45		office/word	no	no	3007.doc	doc	ara fas	mgholami	REmam
	2009-10-12 17:10:45		office/word	no	no	3007.doc	doc	ara fas	REmam	
	2009-10-11 08:40:53		office/word	no	no	[illegible].doc	doc	ara	emam	Computer
	2009-10-11 08:40:53		office/word	no	no	[illegible].doc	doc	ara	Computer2	
	2009-10-13 00:33:52		office/word	no	no			ara fas	REmam	REmam
	2009-10-12 20:16:42		office/word	no	no	Bayan.doc	doc	ara fas	mohamad	mali
	2009-10-12 20:16:42		office/word	no	no	Bayan.doc	doc	ara fas	mali	
	2009-10-12 14:21:10		office/word	no	no	Table.doc	doc	ara	R-Ghanavi	By PARHA
	2009-10-12 14:21:10		office/word	no	no	Table.doc	doc	ara	By PARHAM © RJB270	
	2009-10-12 16:15:04		office/word	no	no	Bayan.doc	doc	ara fas	mohamad	mali
	2009-10-12 16:15:04		office/word	no	no	Bayan.doc	doc	ara fas	mali	
	2009-10-12 12:46:35		office/word	no	no			ara fas	Mortazavi	Mortazavi

Page 1 of 4 Page Size: 30 (Max. 200 rows per page) Displaying 1 - 30 of 114

Email Addrs/Phone Numbers/Login etc

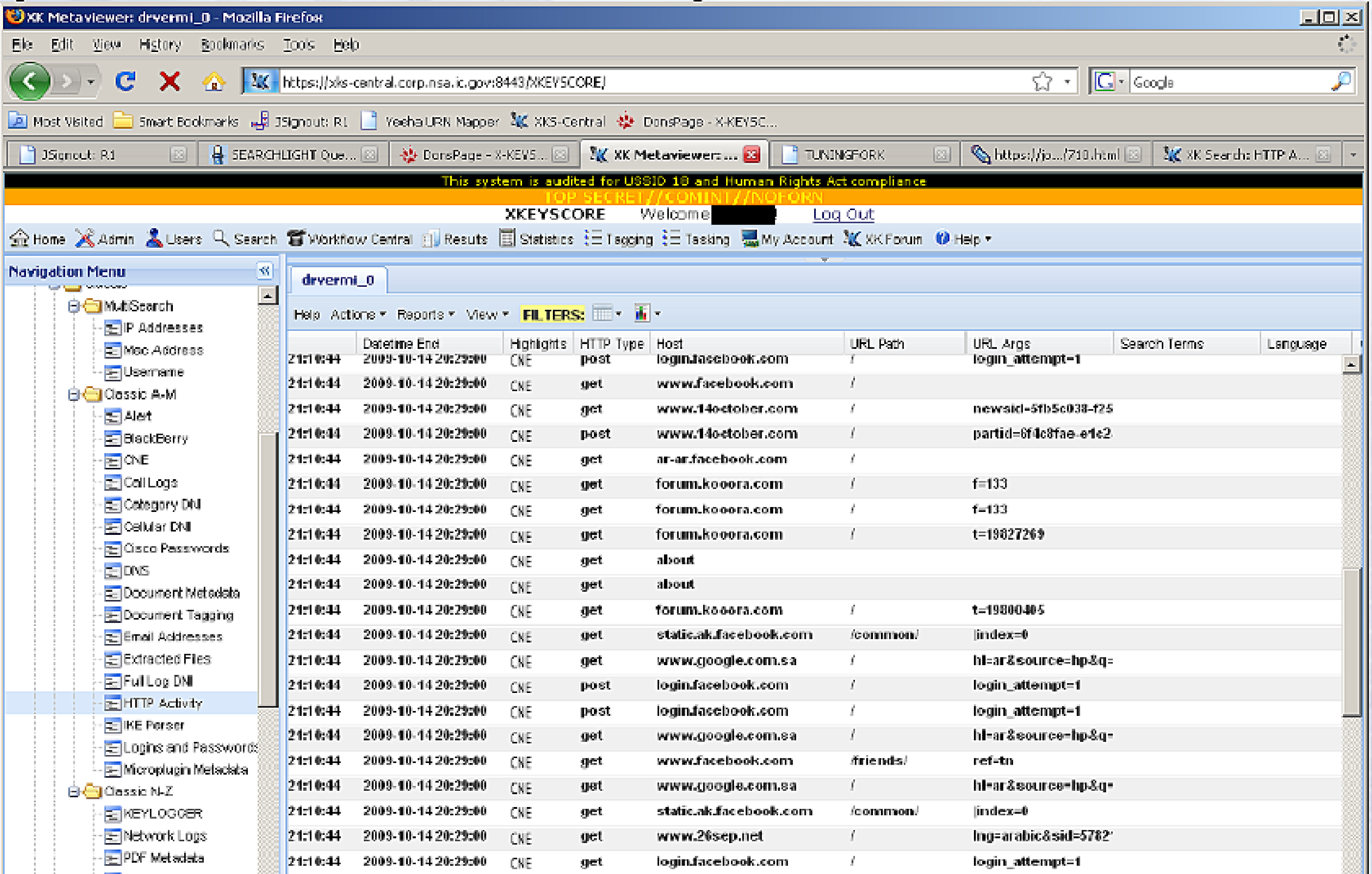

XK Metaviewer: dasteen_20091013_s5 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/
Most Visited Smart Bookmarks JSignout R1 Yeeha URN Mapper XKS-Central DonsPage - X-KEYSC...
JSignout R1 SEARCHLIGHT Quer... DonsPage - X-KEYS... XK Metaviewer:... 74314 (dia ice the ... TUNINGFORK https://p.../710.html XK Results
This system is audited for USSID 18 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
SIP
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
Link Summarization
Tagging
Local Tagging
Job Extractor
Tasking
VoIP Tasking
My Account
Histogram: @Domain
Histogram Grid
Clear Selection
Histogram of: @Domain (Click Bar to Filter)
400
300
200
100
0
452
158
3
3
3
3
3
1
1
ssp.gob.mx
pfp.local
bml.megfoc...
businessmonit...
ims-ms-daemon
mail.norinco.cn
zhenhuaoil.com
inwind.it
steele-net.cu
Pivot: Casenotation
Clear Selection
MX.RFI (610)
CC CHS (15)
MILCAUT (2)
dasteen_20091013_s5
Help Actions Reports View FILTERS:
Page 1 of 11 Page size 70 (Max 100 rows per page)
Displaying 1 - 70 of 672
dasteen_07301400012554306S6_1
This system is audited for USSID 18 and Human Rights Act compliance
TOP SECRET//COMINT//NOFORN
Done
xks-central.corp.nsa.ic.gov:8443

Email User Name	Datetime	Highlights	@Domain	Subject	Chain
[redacted]	2009-10-10 05:15:10	CNE	mail.norinco.cn	2840 senior contacts in India for zhe	0kqe00g01mrdlk@mail.norinco.cn&kate.strut
[redacted]	2009-10-10 05:15:10	CNE	businessmonitor.cor	2840 senior contacts in India for zhe	0kqe00g01mrdlk@mail.norinco.cn&kate.strut
[redacted]	2009-10-10 05:15:10	CNE	bml.megfocus.com	2840 senior contacts in India for zhe	0kqe00g01mrdlk@mail.norinco.cn&kate.strut
[redacted]	2009-10-10 05:15:10	CNE	zhenhuaoil.com	2840 senior contacts in India for zhe	0kqe00g01mrdlk@mail.norinco.cn&kate.strut
[redacted]	2009-10-10 05:15:10	CNE	ims ms daemon	2840 senior contacts in India for zhe	0kqe00g01mrdlk@mail.norinco.cn&kate.strut
[redacted]	2009-10-12 08:29:00		steele net.cu	2010 swiss rolex	3djuliette@steele net.cu&bvlgari@inwind.it
[redacted]	2009-10-12 08:29:00		inwind.it	2010 swiss rolex	3djuliette@steele net.cu&bvlgari@inwind.it
[redacted]	2009-10-11 08:38:53	CNE	ssp.gob.mx	101009 EII LA PAZ, BAJA CALIFORNI/	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:53	CNE	pfp.local	101009 EII MEXICALI, BAJA CALIFOR	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:53	CNE	ssp.gob.mx	101009 EII MEXICALI, BAJA CALIFOR	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:53	CNE	ssp.gob.mx	101009 EII LA PAZ, BAJA CALIFORNI/	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:53	CNE	ssp.gob.mx	101009 EII LA PAZ, BAJA CALIFORNI/	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:50	CNE	ssp.gob.mx	101009 EII CIUDAD JUÁREZ, CHIHUAH	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:50	CNE	ssp.gob.mx	101009 EII CIUDAD JUÁREZ, CHIHUAH	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:53	CNE	pfp.local	101009 EII LA PAZ, BAJA CALIFORNI/	dgie1.analisis@pfp.local&eduardo.argote@s
[redacted]	2009-10-11 08:38:50	CNE	ssp.gob.mx	101009 EII GALEANA, CHIHUAHUA, SE	dgie1.analisis@pfp.local&eduardo.argote@s

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

HTTP Activity (FOGGYBOTTOM)

NEW!!



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

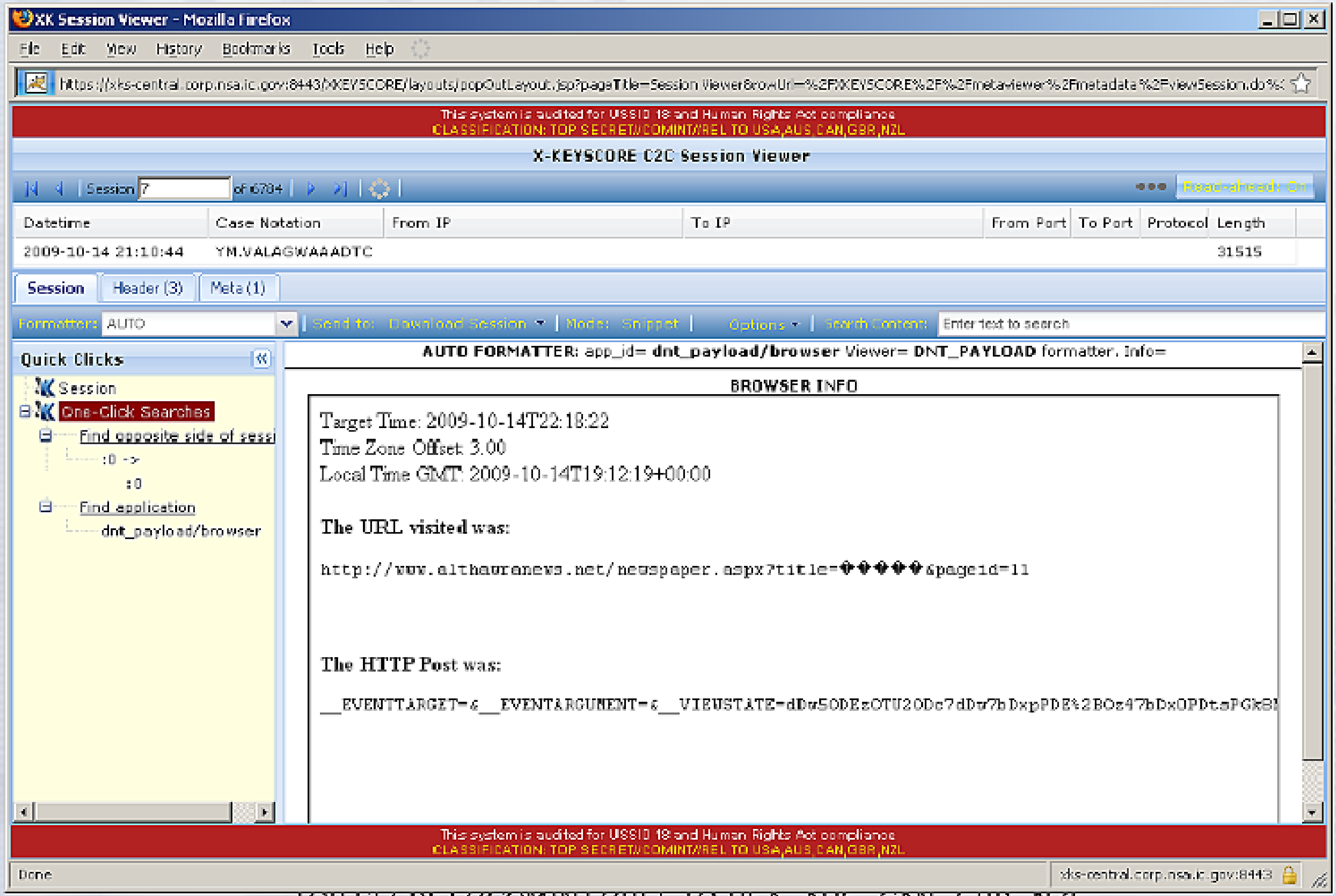
TOP SECRET//COMINT//NOFORN

XKEYSCORE Welcome [redacted] Log Out

	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.kooora.com	/	f=133		
21:10:44	2009-10-14 20:29:00	CNE	get	forum.kooora.com	/	f=133		
21:10:44	2009-10-14 20:29:00	CNE	get	forum.kooora.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.kooora.com	/	t=19800405		
21:10:44	2009-10-14 20:29:00	CNE	get	static.ak.facebook.com	/common/	jindex=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/	jindex=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)

NEW!!



XK Session Viewer - Mozilla Firefox
File Edit View History Bookmarks Tools Help

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

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

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

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

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.althauranews.net/newspaper.aspx?title=�����&pageid=11
```

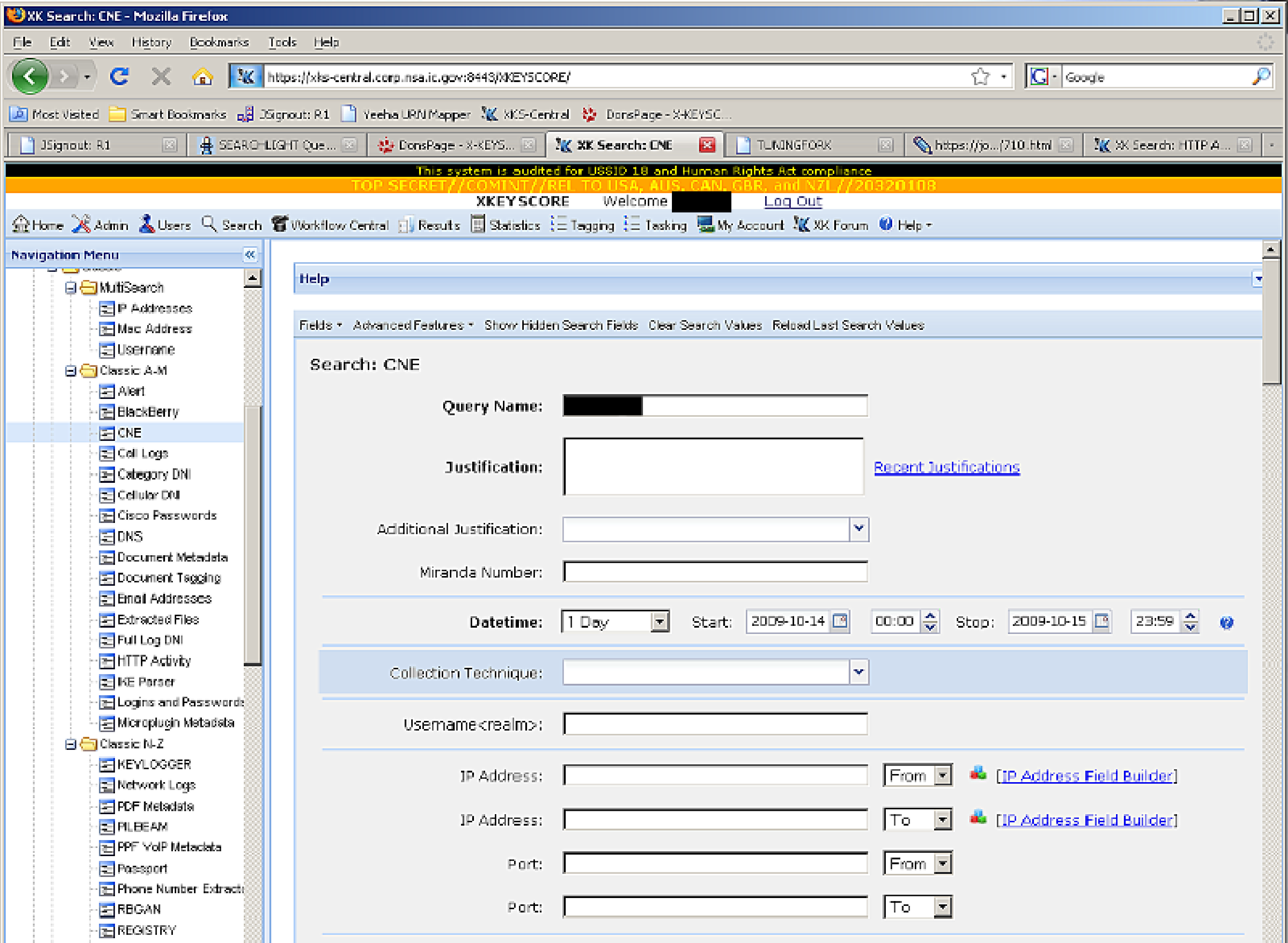
The HTTP Post was:

```
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=dDw5ODEzOTU2ODc7dDw7bDxpPDE%2BOz47bDxOPDtsPGk8
```

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

CNE
Specific Searches

CNE Search



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 [redacted] Log Out

Search: CNE

Query Name: [redacted]

Justification:

Additional Justification:

Miranda Number:

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

Collection Technique:

Username<realm>:

IP Address: From

IP Address: To

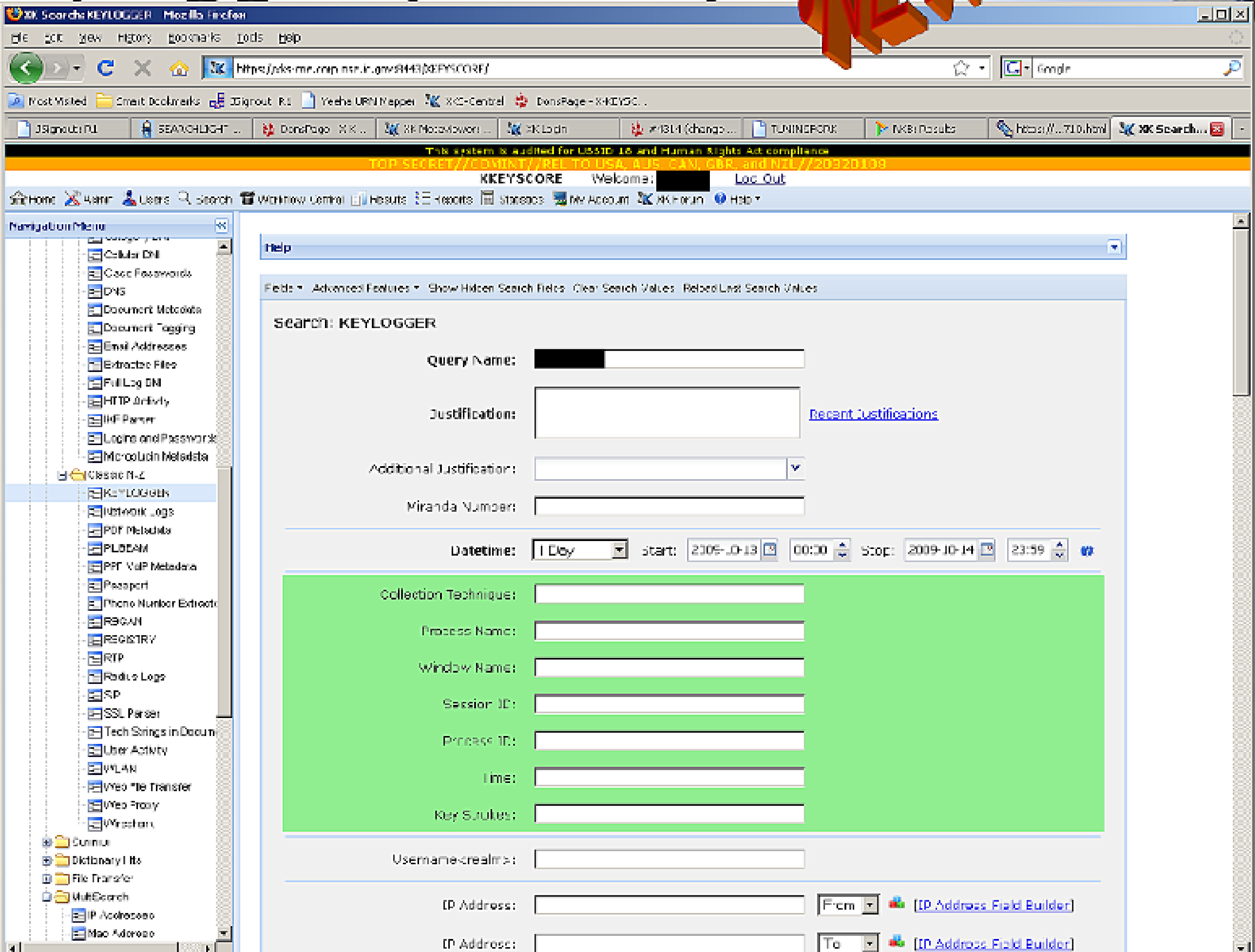
Port: From

Port: To

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

Keylogger (search)

NEW!!



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: [redacted] Log Out

Search: KEYLOGGER

Query Name: [redacted]

Justification:

Additional Justification:

Miranda Number:

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

Collection Technique:

Process Name:

Window Name:

Session ID:

Process ID:

Time:

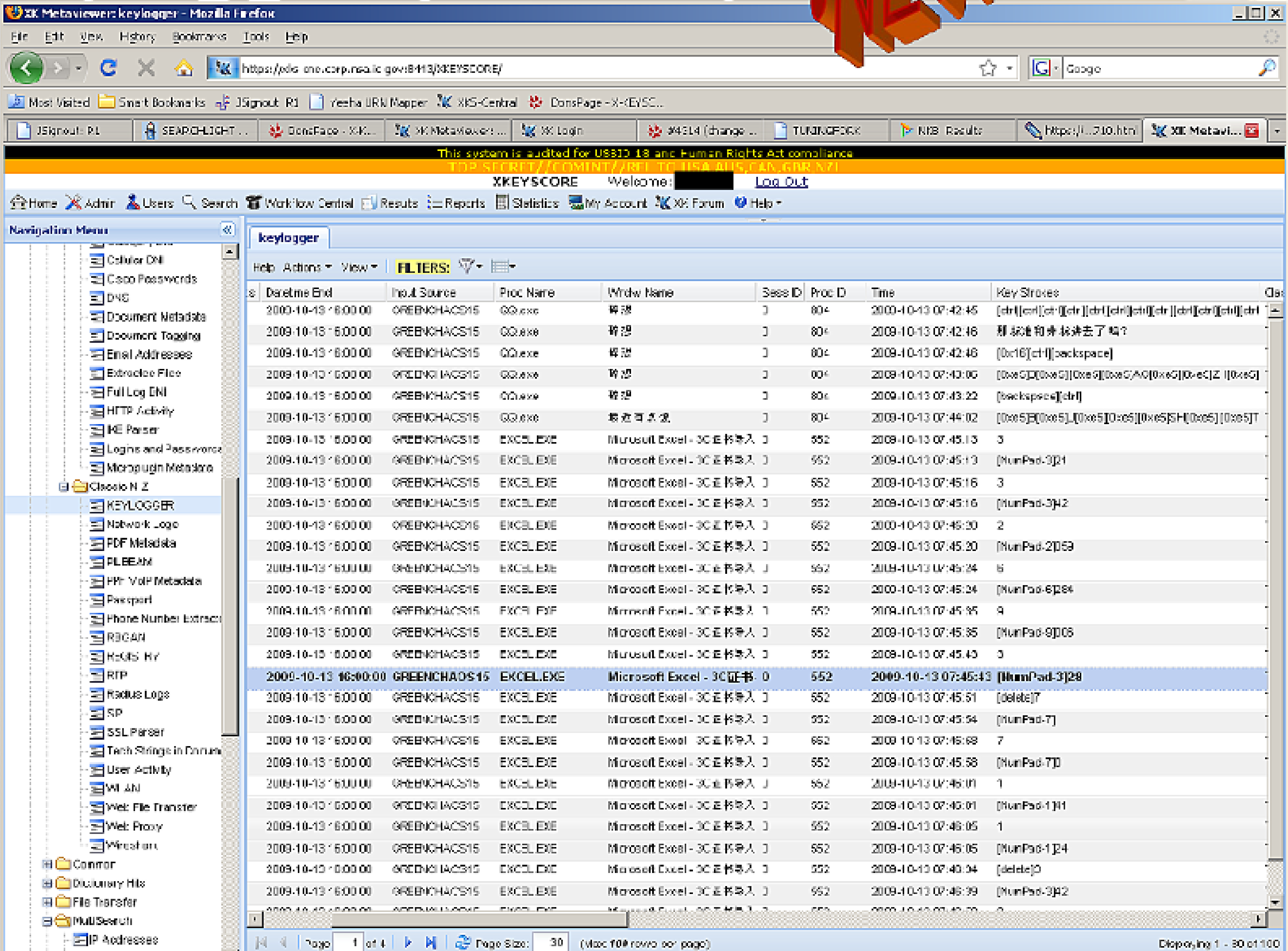
Key Strokes:

Username-realm:

IP Address: From

IP Address: To

Keylogger (results)



XK Metaviewer: keylogger - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://pkls one.corp.nsa.ic.gov:8443/XKEYSCORE/
Google
Most Visited · Smart Bookmarks · JSignout R1 · Yeeha URN Mapper · XKS-Central · DonsPage - X-KEYSC...
JSignout R1 · SEARCHLIGHT ... · DonsPage - X-K... · XK Metaviewer ... · XK Login · #4314 (change ... · TUNINGFORK · NKB Results · https://...710.htm · XK Metavi...

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

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

XKEYSCORE Welcome: [redacted] Log Out

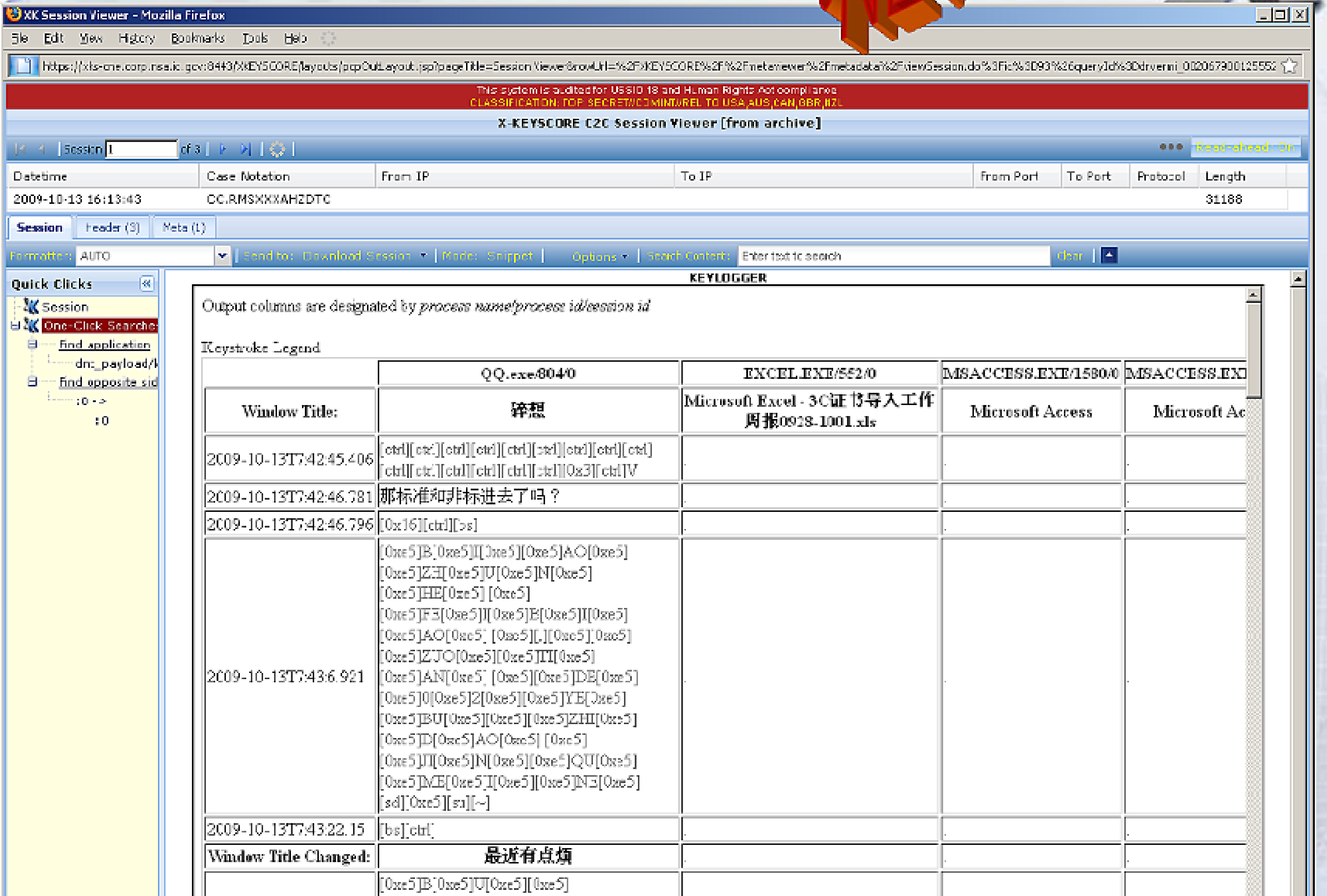
Home · Admin · Users · Search · Workflow Central · Results · Reports · Statistics · My Account · XK Forum · Help
Navigation Menu
Cellular DNI
Cisco Passwords
DNS
Document Metadata
Document Tagging
Email Addresses
Extracted Files
Full Log DNI
HTTP Activity
IKE Parser
Logins and Passwords
Micropugin Metadata
Classic N-Z
KEYLOGGER
Network Logs
PDF Metadata
PLBEAM
PPP VoIP Metadata
Passport
Phone Number Extract
RBCAN
ReGIS HY
RTP
Radius Logs
SIP
SSL Parser
Tech Strings in Docum
User Activity
WLAN
Web File Transfer
Web Proxy
Wireshark
Common
Dictionary Hits
File Transfer
MultiSearch
IP Addresses
keylogger
Help · Actions · View · FILTERS:

Datetime End	Input Source	Proc Name	Window Name	Sess ID	Proc ID	Time	Key Strokes
2009-10-13 16:00:00	GREENCHAOS15	QQ.exe	[illegible]	0	804	2009-10-13 07:42:45	[ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl
2009-10-13 16:00:00	GREENCHAOS15	QQ.exe	[illegible]	0	804	2009-10-13 07:42:46	那[illegible]去了吗?
2009-10-13 16:00:00	GREENCHAOS15	QQ.exe	[illegible]	0	804	2009-10-13 07:42:46	[0x16][ctrl][backspace]
2009-10-13 16:00:00	GREENCHAOS15	QQ.exe	[illegible]	0	804	2009-10-13 07:43:06	[0xe5]D[0xe5][0xe5][0xe5]AO[0xe5][0xe5]Z I[0xe5]
2009-10-13 16:00:00	GREENCHAOS15	QQ.exe	[illegible]	0	804	2009-10-13 07:43:22	[backspace][ctrl]
2009-10-13 16:00:00	GREENCHAOS15	QQ.exe	[illegible]	0	804	2009-10-13 07:44:02	[0xe5]B[0xe5]L[0xe5][0xe5][0xe5]SH[0xe5][0xe5]T
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:13	3
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:13	[NumPad-3]21
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:16	3
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:16	[NumPad-3]42
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:20	2
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:20	[NumPad-2]059
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:24	6
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:24	[NumPad-6]284
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:35	9
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:35	[NumPad-9]006
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:43	3
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书	0	552	2009-10-13 07:45:43	[NumPad-3]28
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:51	[delete]7
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:54	[NumPad-7]
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:58	7
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:45:58	[NumPad-7]0
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:46:01	1
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:46:01	[NumPad-1]41
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:46:05	1
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:46:05	[NumPad-1]24
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:46:34	[delete]0
2009-10-13 16:00:00	GREENCHAOS15	EXCEL.EXE	Microsoft Excel - 3C证书导入	0	552	2009-10-13 07:46:39	[NumPad-3]42

Page 1 of 4 Page Size: 30 (max 100 rows per page) Displaying 1 - 30 of 100

Keylogger (session vi

NEW!!



https://xks-cne.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaviewer%2Fmetadata%2FviewSession.do%3Fid%3D93%26queryId%3Ddrverni_00206790125552

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]

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2009-10-13 16:13:43	CC.RMSXXXAHZDTC						31188

KEYLOGGER

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

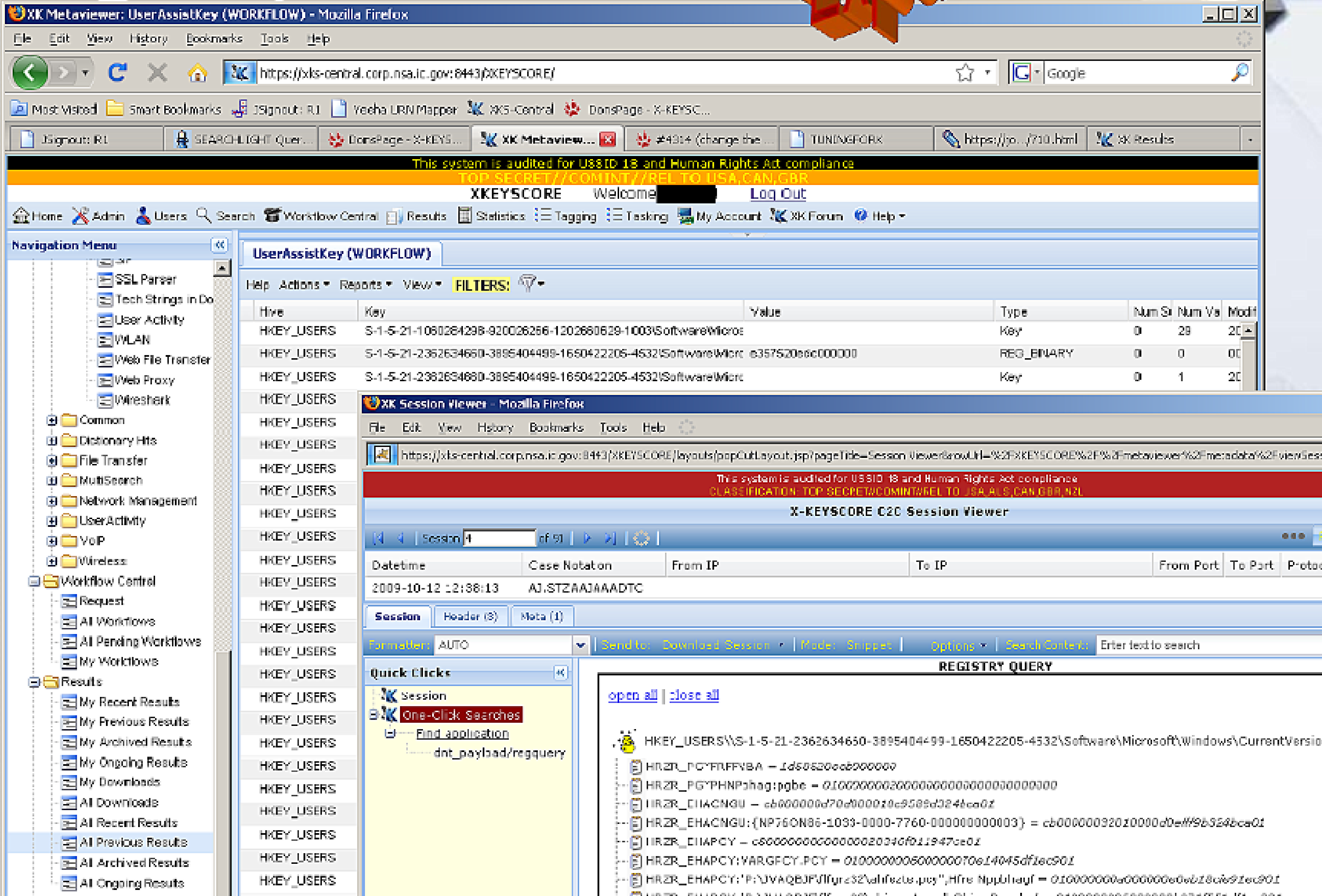
Keystroke Legend

	QQ.exe/804/0	EXCEL.EXE/552/0	MSACCESS.EXE/1580/0	MSACCESS.EXI
Window Title:	**猝想**	**Microsoft Excel - 3C证书导入工作周报0928-1001.xls**	**Microsoft Access**	**Microsoft Ac**
2009-10-13T7:42:45.406	[ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][ctrl] [ctrl][ctrl][ctrl][ctrl][ctrl][ctrl][0x3][ctrl]V	.	.	.
2009-10-13T7:42:46.781	那标准和非标进去了吗？	.	.	.
2009-10-13T7:42:46.796	[0x16][ctrl][bs]	.	.	.
2009-10-13T7:43:6.921	[0xe5]B[0xe5]I[0xe5][0xe5]AO[0xe5] [0xe5]ZH[0xe5]U[0xe5]N[0xe5] [0xe5]HE[0xe5] [0xe5] [0xe5]F3[0xe5]I[0xe5]B[0xe5]I[0xe5] [0xe5]AO[0xe5] [0xe5][,][0xe5][0xe5] [0xe5]ZJO[0xe5][0xe5]TI[0xe5] [0xe5]AN[0xe5] [0xe5][0xe5]DE[0xe5] [0xe5]0[0xe5]2[0xe5][0xe5]YE[0xe5] [0xe5]BU[0xe5][0xe5][0xe5]ZHI[0xe5] [0xe5]D[0xe5]AO[0xe5] [0xe5] [0xe5]JI[0xe5]N[0xe5][0xe5]QU[0xe5] [0xe5]ME[0xe5]I[0xe5][0xe5]NE[0xe5] [sd][0xe5][sa][~]	.	.	.
2009-10-13T7:43:22.15	[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

Registry

Expanded!



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

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

XKEYSCORE Welcome [redacted] Log Out

Hive	Key	Value	Type	Num Sı	Num Va	Modi
HKEY_USERS	S-1-5-21-1060284298-920026266-1202660629-1003\Software\Micros		Key	0	29	20
HKEY_USERS	S-1-5-21-2362634660-3895404499-1650422205-4532\Software\Micrc	e357520e6c000000	REG_BINARY	0	0	00
HKEY_USERS	S-1-5-21-2362634660-3895404499-1650422205-4532\Software\Micrc		Key	0	1	20
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						
HKEY_USERS						

XK Session Viewer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaviewer%2Fmetadata%2FviewSes

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

Session 4 of 51

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protoc
2009-10-12 12:38:13	AJ.STZAAJAAADTC					

REGISTRY QUERY

open all | close all

```
HKEY_USERS\\S-1-5-21-2362634650-3895404499-1650422205-4532\Software\Microsoft\Windows\CurrentVersio
  HRZR_PGYFRFFVBA = 1d58520eeb000000
  HRZR_PGYPHNPbhag:pgbe = 01000000020000000000000000000000
  HRZR_EHACNGU = cb000000d70a000010c9589d324bca01
  HRZR_EHACNGU:{NP76ON86-1033-0000-7760-000000000003} = cb0000003201000d0eff9b324bca01
  HRZR_EHAPCY = c6000000000000020346f011947ce01
  HRZR_EHAPCY:VARGFCY.PCY = 01000000060000070e14045df1ec901
  HRZR_EHAPCY:'P:\JVAQBJF\flfgrz32\ahfrzie.pcy",Hfre Nppbhagf = 01000000a000000e0eb18cfe91ec901
```

KEYSCORE

Wrap Up

Payloads Handled

Parsing	Tailored Viewing
• Browser Info	yes
• Collected Files	standard XKS view
• Directory Walks	yes
• Drive Listings	xml
• Ipconfig	xml
• Keylogger	yes
• Process Lists	xml
• Registry	yes
• System Survey (partial)	xml

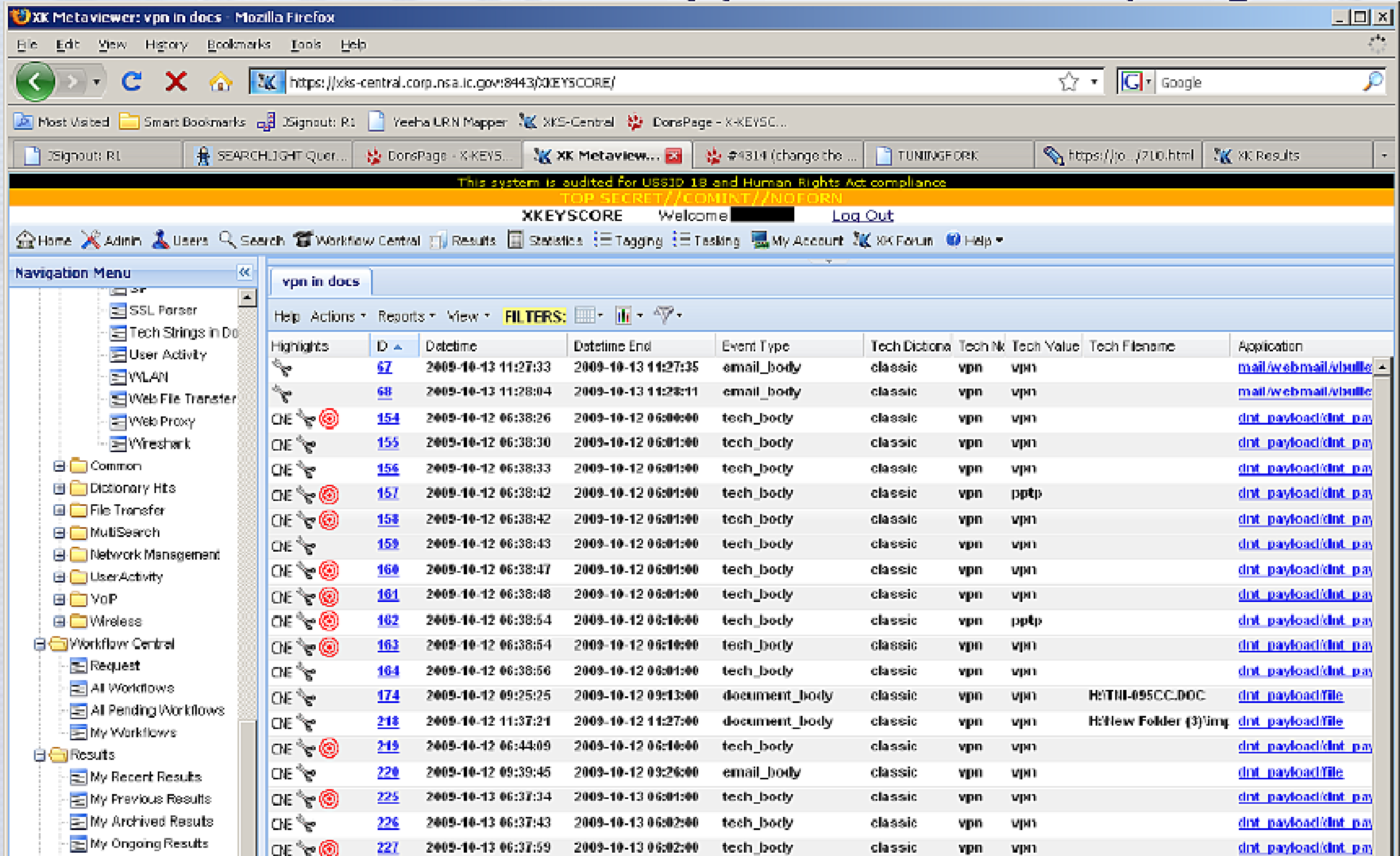
Other Payloads

- 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

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

Tech Strings in Documents

- Catchall for data types without plugins


XK Metaviewer: vpn in docs - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Smart Bookmarks JSignout: R1 Yeeha URN Mapper XKS-Central DonsPage - X-KEYSC...
JSignout: R1 SEARCHLIGHT Quer... DonsPage - X-KEYS... XK Metaview... #4314 (change the ... TUNINGFORK https://jo.../710.html XK Results
Home Admin Users Search Workflow Central Results Statistics Tagging Tasking My Account XK Forum Help
Navigation Menu
SF
SSL Parser
Tech Strings in Do
User Activity
VVLAN
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:

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

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

TOP SECRET//COMINT//NOFORN

XKEYSCORE Welcome [redacted] Log Out

Highlights	ID	Datetime	Datetime End	Event Type	Tech Dictiona	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/vbulle
	68	2009-10-13 11:28:04	2009-10-13 11:28:11	email_body	classic	vpn	vpn		mail/webmail/vbulle
CNE	154	2009-10-12 06:38:26	2009-10-12 06:00:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	155	2009-10-12 06:38:30	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	156	2009-10-12 06:38:33	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	157	2009-10-12 06:38:42	2009-10-12 06:01:00	tech_body	classic	vpn	pptp		dnt_payload/dnt_pay
CNE	158	2009-10-12 06:38:42	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	159	2009-10-12 06:38:43	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	160	2009-10-12 06:38:47	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	161	2009-10-12 06:38:48	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	162	2009-10-12 06:38:54	2009-10-12 06:10:00	tech_body	classic	vpn	pptp		dnt_payload/dnt_pay
CNE	163	2009-10-12 06:38:54	2009-10-12 06:10:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	164	2009-10-12 06:38:56	2009-10-12 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	174	2009-10-12 09:25:25	2009-10-12 09:13:00	document_body	classic	vpn	vpn	H:\TNI-095CC.DOC	dnt_payload/file
CNE	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
CNE	219	2009-10-12 06:44:09	2009-10-12 06:10:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	220	2009-10-12 09:39:45	2009-10-12 09:26:00	email_body	classic	vpn	vpn		dnt_payload/file
CNE	225	2009-10-13 06:37:34	2009-10-13 06:01:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	226	2009-10-13 06:37:43	2009-10-13 06:02:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay
CNE	227	2009-10-13 06:37:59	2009-10-13 06:02:00	tech_body	classic	vpn	vpn		dnt_payload/dnt_pay

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 Explotation

XKEYSCORE

Questions?

Blank

NEW!!

- Page