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

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

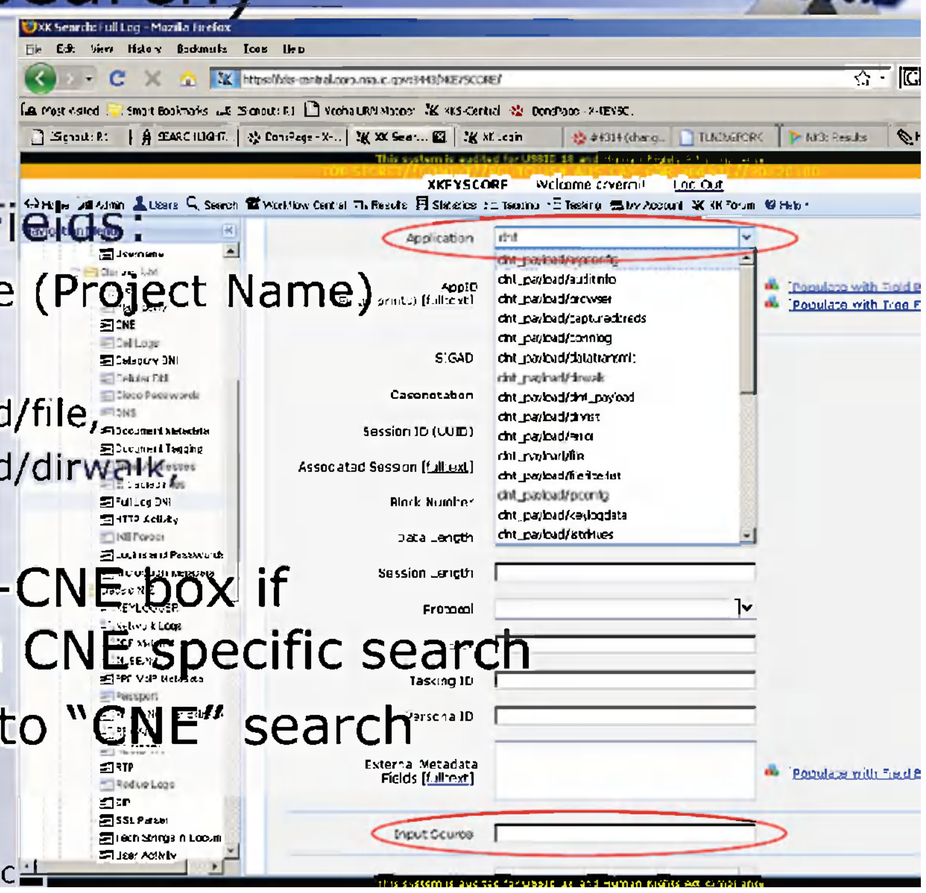
QUERY RESULTS (ad-hoc):
userxxx email_addresses 22/10421 Iran NPS Domains userxxx_0808493001253628218_1
f652856 document_metadata 11/1053 f652856_0 f652856_0631781001253611176_1
useryyy tech 2/2 Iran Tech Search useryyy_0303242001253646149_1
...

Distribution of Searches by type:
email_addresses: 7
extracted_files: 32
full_log: 5
document_metadata: 6
phone_number: 1
tech: 4
registry: 5

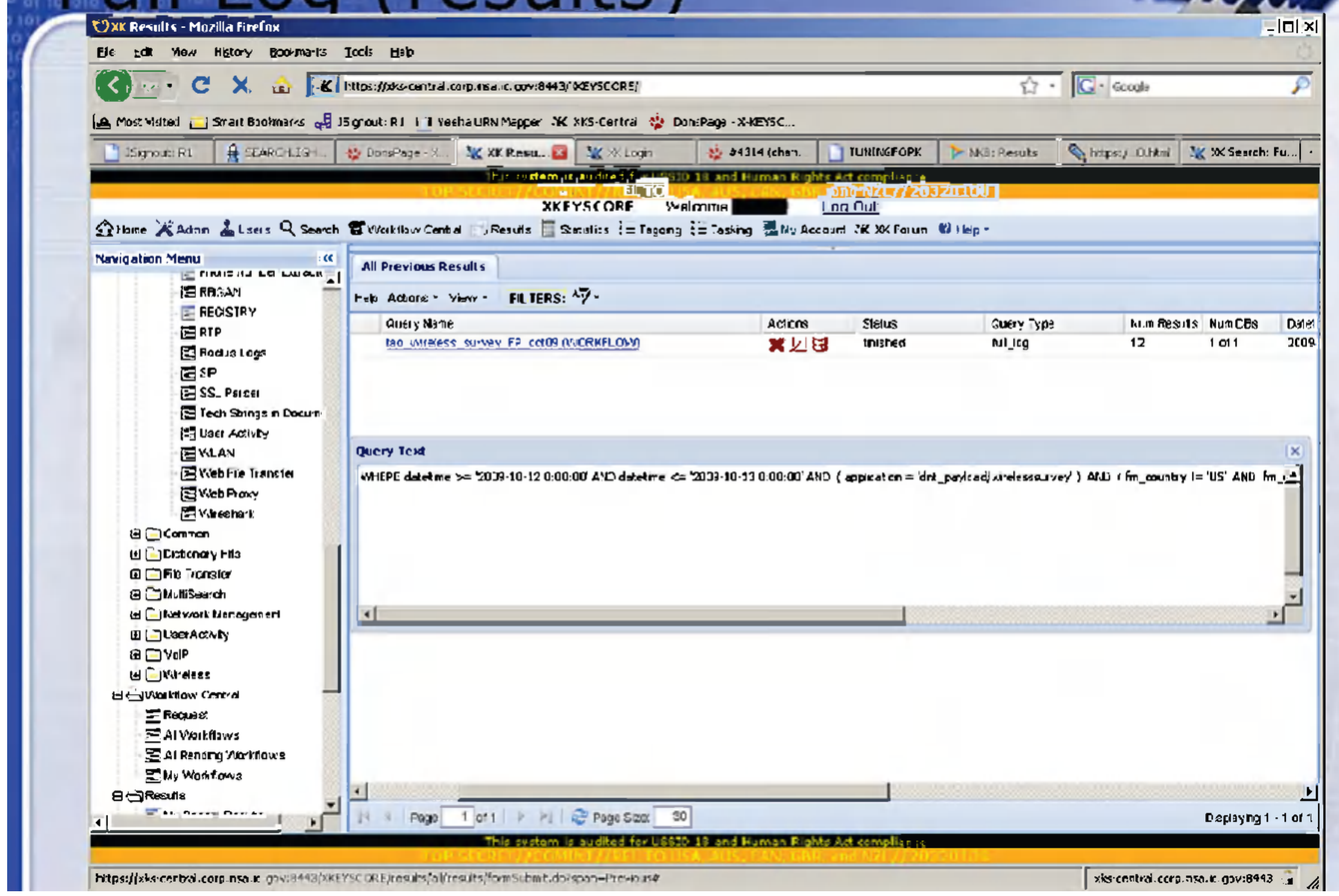
XKEYSCORE Searches (live demo)

Full Log (search)

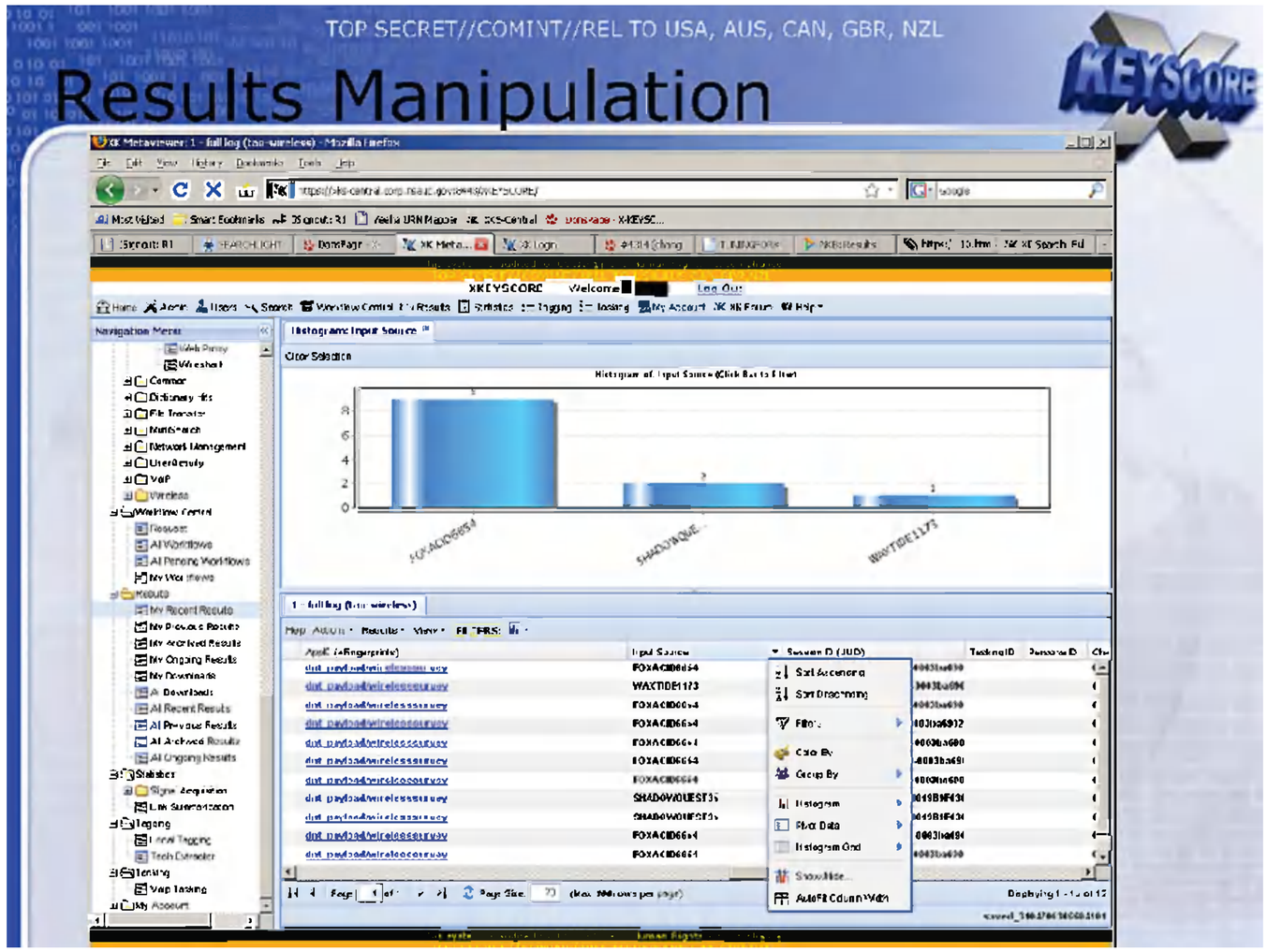
- Often Used Fields:
  - Input Source (Project Name)
  - Application
    - dnt_payload/file,
    - dnt_payload/dirwalk
    - ...
- Limit to XKS-CNE box if performing a CNE specific search
- Very similar to "CNE" search

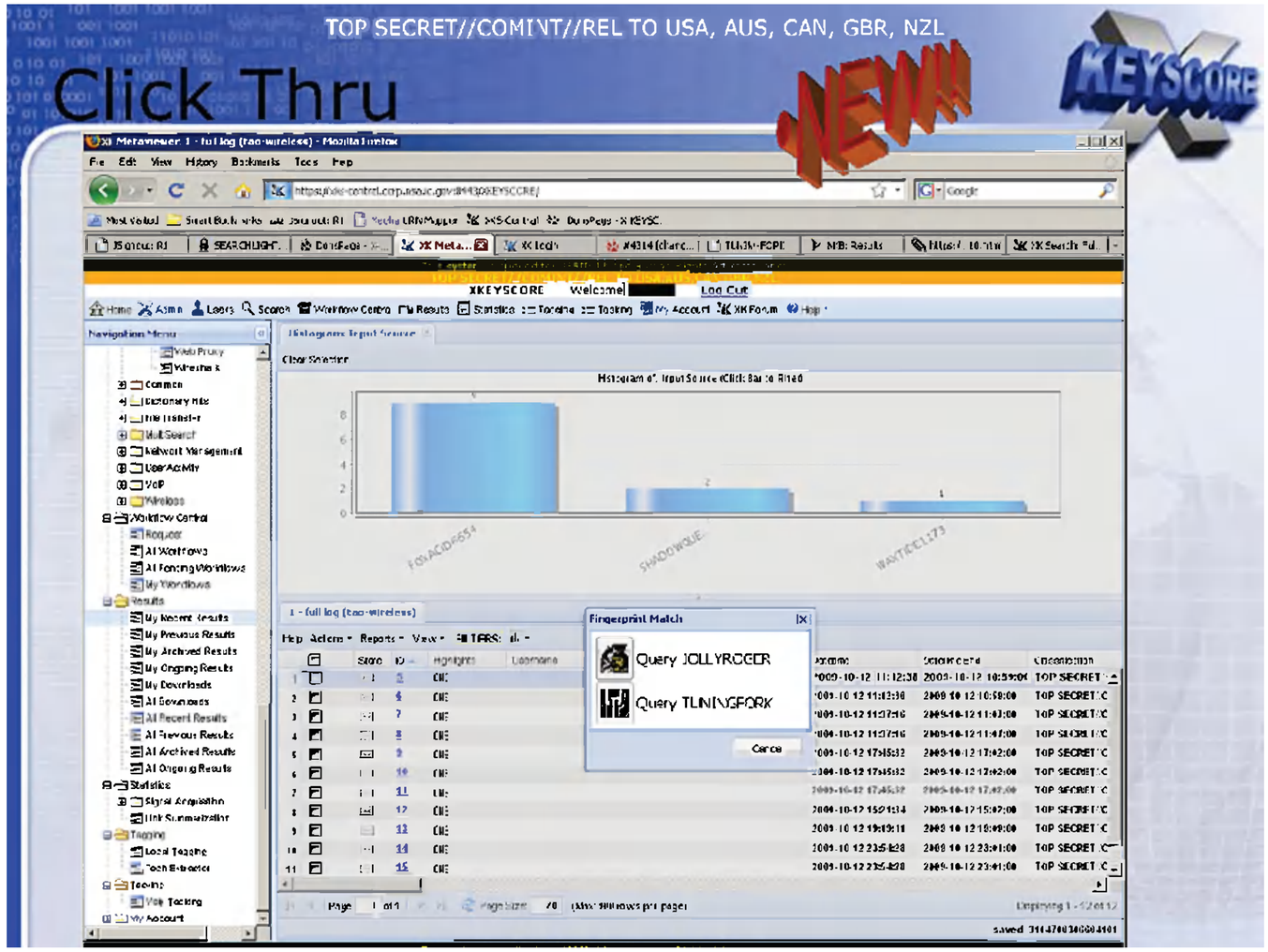


Full Log (results)

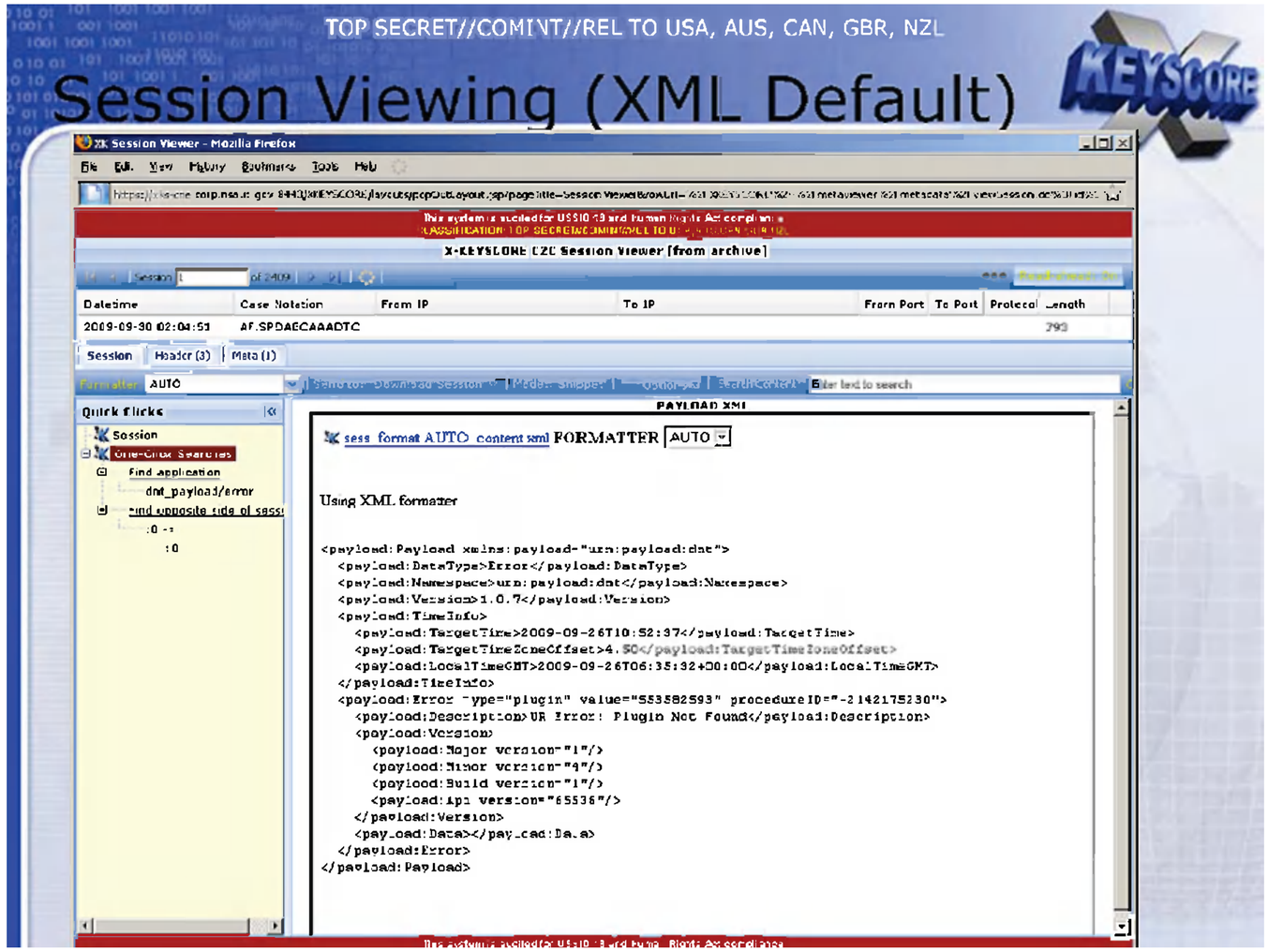


Results Manipulation



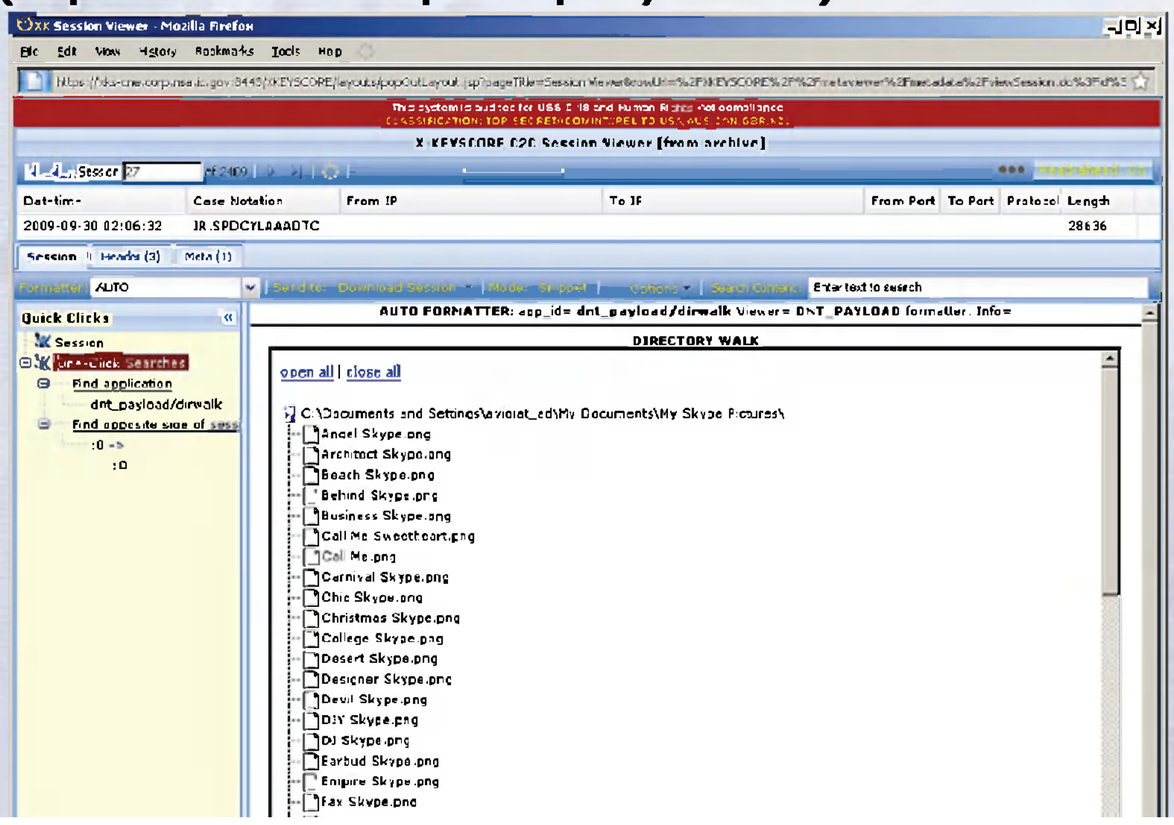

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Click Thru
NEW!!
KEYSCORE
XKEYSCORE
Log Out
Fingerprint Match
Query JOLLYROGER
Query TLINKSFORK
Cancel

Session Viewing (XML Default)



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

Session Viewing (Specialized per payload)



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

Session Viewing (CCDF Headers)

XK Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

X KEYSCORE C2C Session Viewer [from archive]

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

Session | Header (3) | Meta (1)

Selected Header Fields | Raw Header (XML) | Full XKS Header

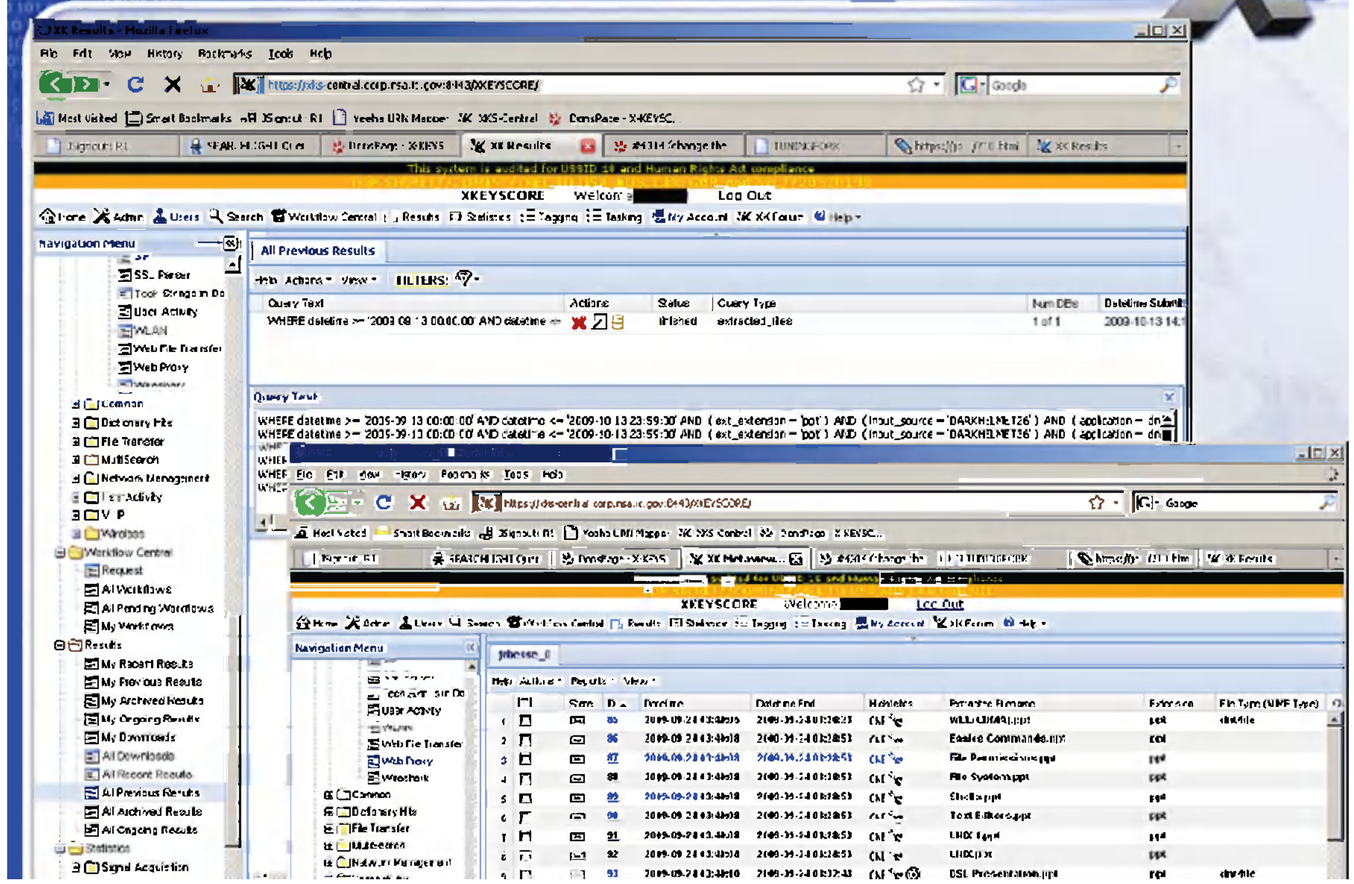
sess_orig.header.xml FORMATTER ALTO

Using XML formatter


```
<ccdf sec:classification="TS" sec:secCoi="COMINT" sec:secNatDissem="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>DTN</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="06c06a66-0124-3b11-1f4d-0019B9F630E7">
    <processingType>collection</processingType>
    <processingCat>collection</processingCat>
    <provider>
      <covername>SHADOWQUEST35</covername>
      <pddq>12</pddq>
      <sigad>US-3101C</sigad>
    </provider>
    <service name="forwarding">
      <parameter name="Target">000000010001328B</parameter>
      <parameter name="SEAGULLFARO_ULID">06c85566-0124-25d7-1f35-0019B9F630E7</parameter>
      <parameter name="TransactionID">000000010001328B.5552.29SR1710209.spouter-2-3.0.final_2014091_0_16up</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

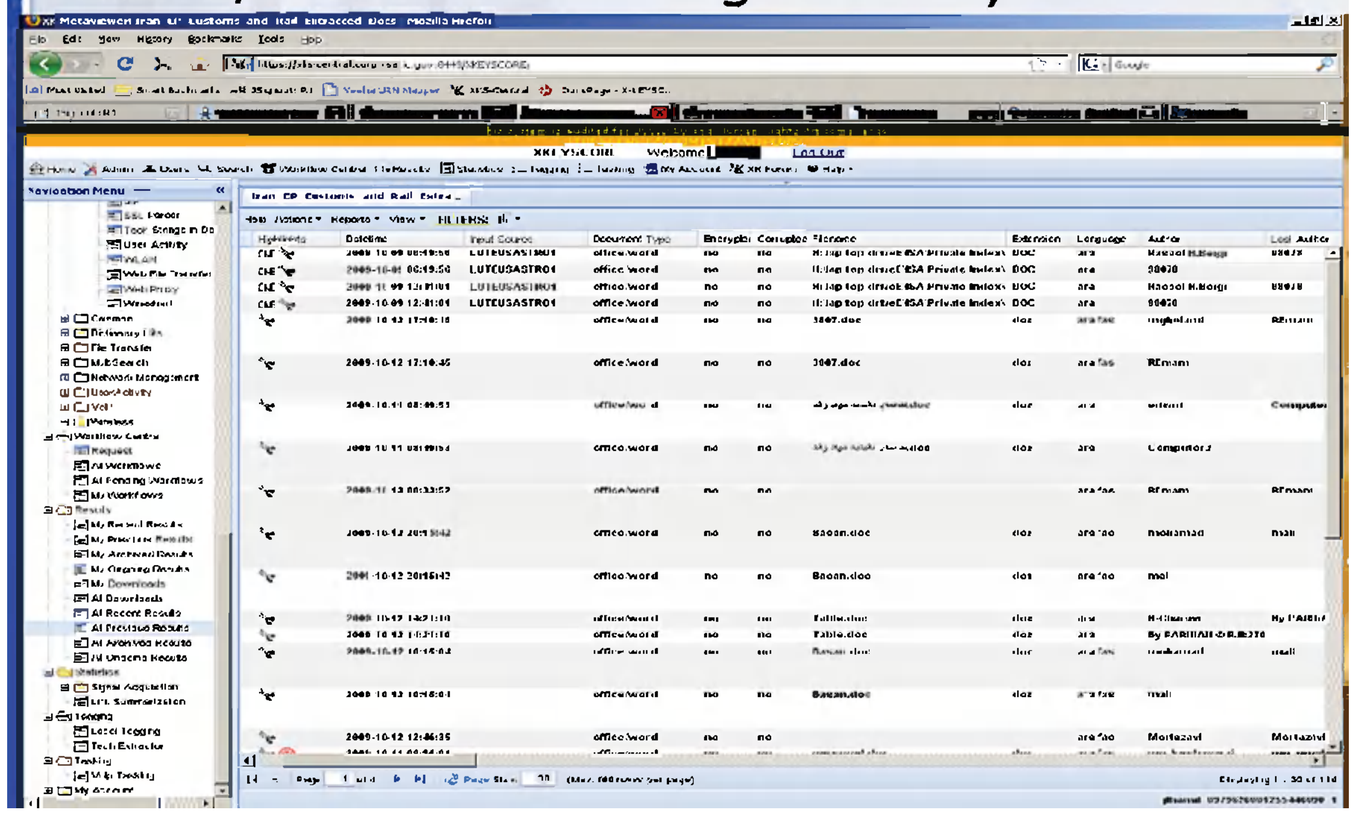
Extracted Files–CNE Specific



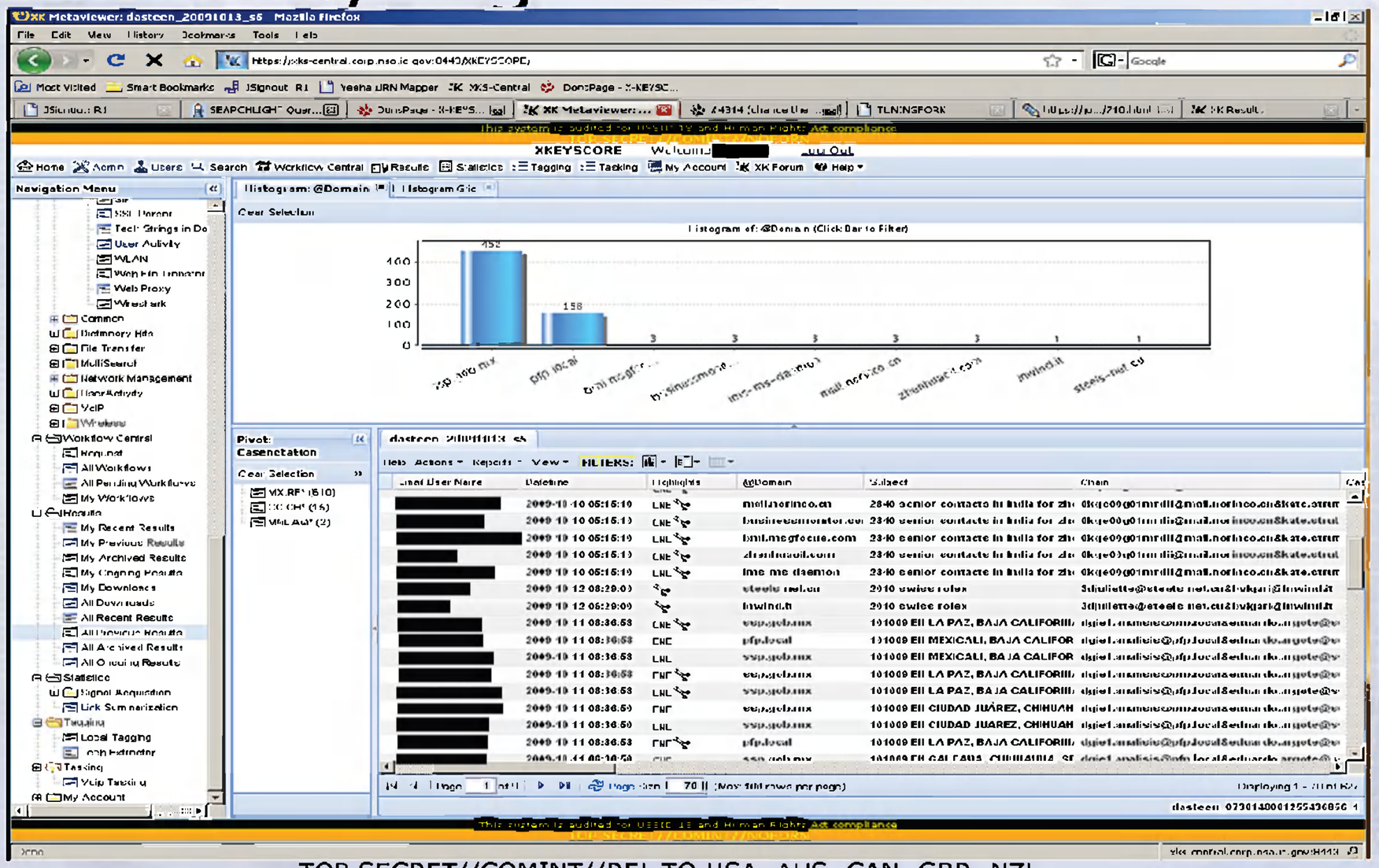
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Document Metadata –

Active/Passive Converged Analysis



Email Addrs/Phone Numbers/Login etc



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

HTTP Activity (FOGGYBOTTOM)

NEW!!

KEYSCORE

XKEYSCORE Welcome [redacted] Log Out

Navigation Menu

MultSearch
- 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

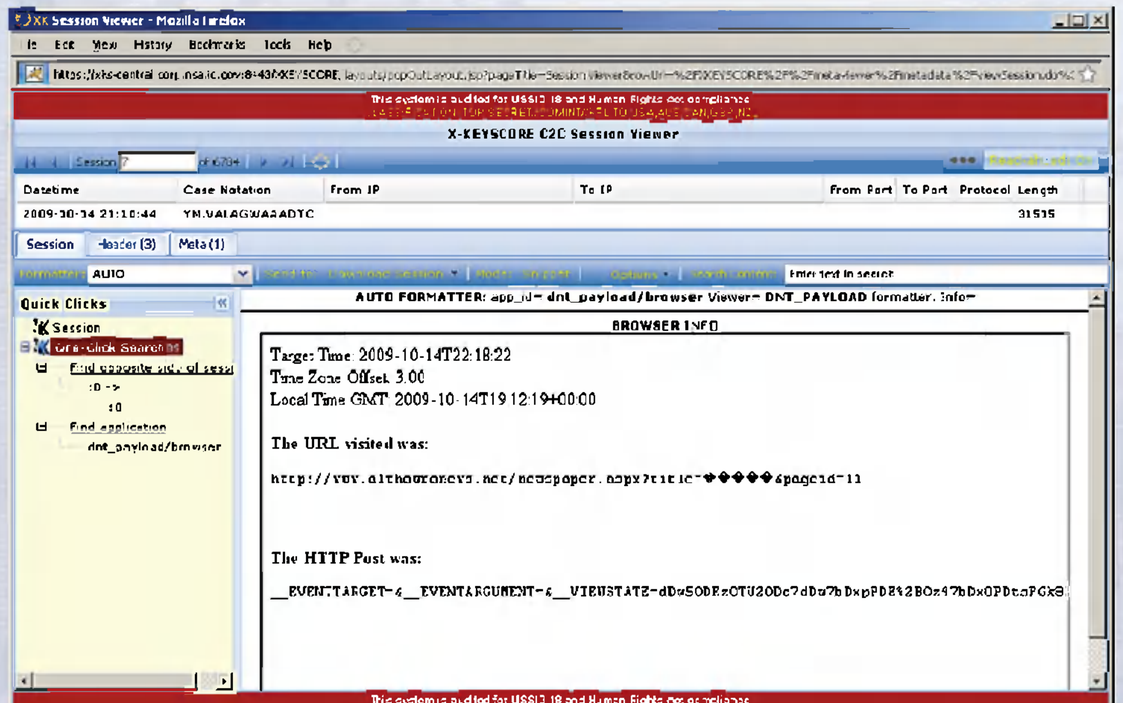
Classic N-Z
- KEYLOGGER
- Network Logs
- PDF Metadata

devermi_0

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=5fb5e038-f25		
21:10:44 2009-10-14 20:29:00	CNE	post	www.14october.com	/	partid=6f1c8fae-e1e2		
21:10:44 2009-10-14 20:29:00	CNE	get	ar-ar.facebook.com	/			
21:10:11 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/	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)

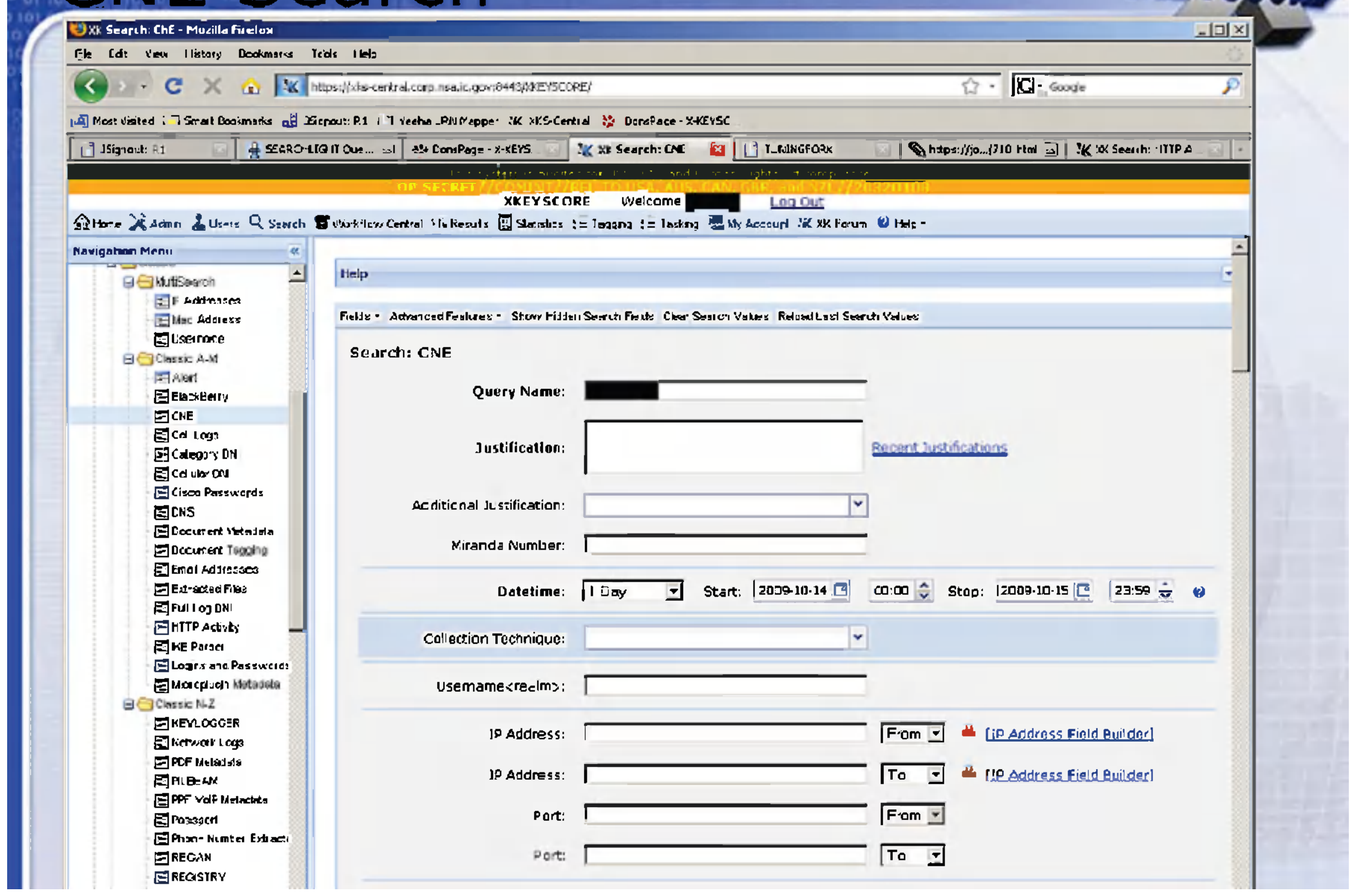
NEW!!



CNE
Specific Searches

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

CNE Search

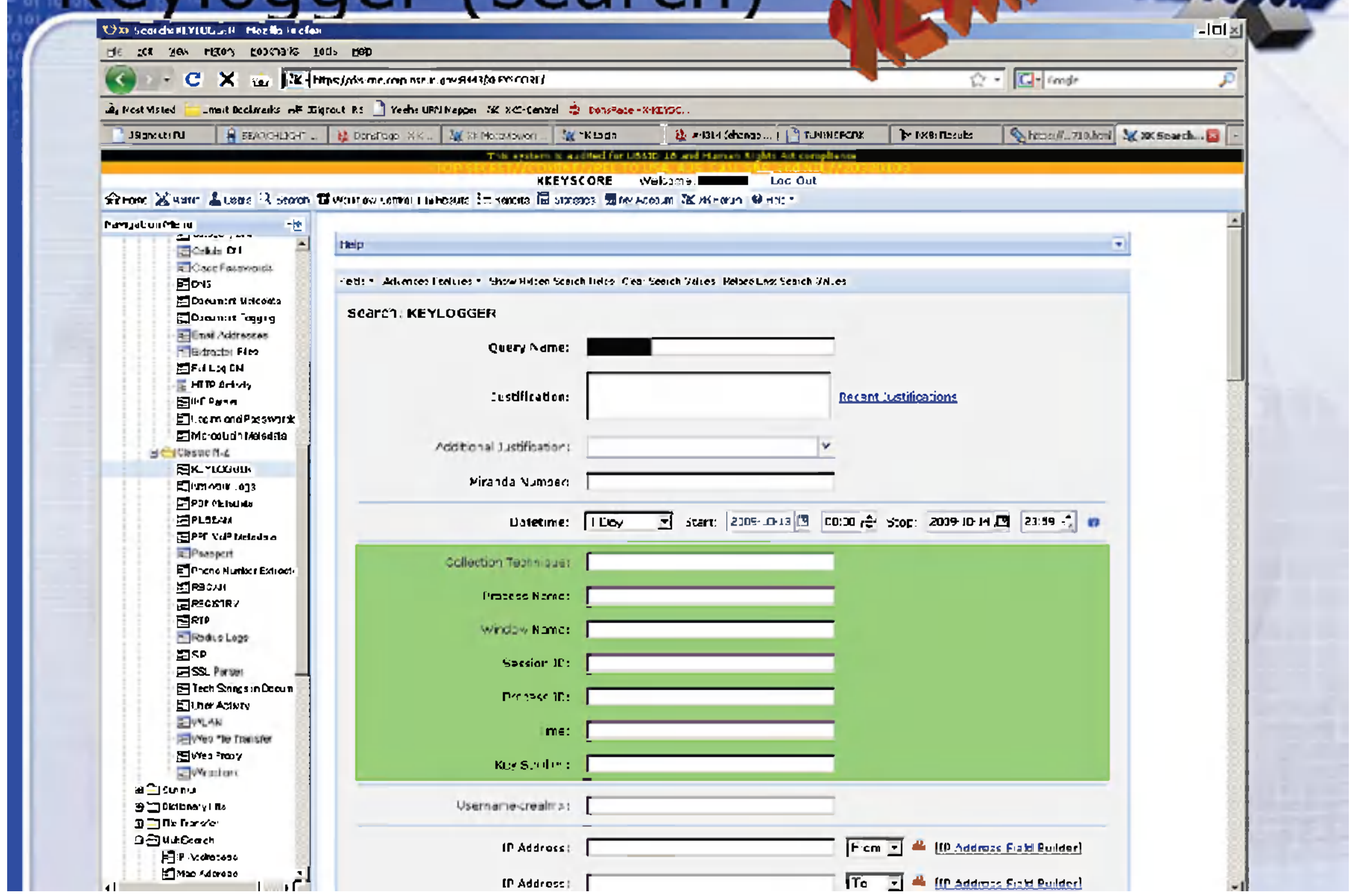


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Keylogger (search)

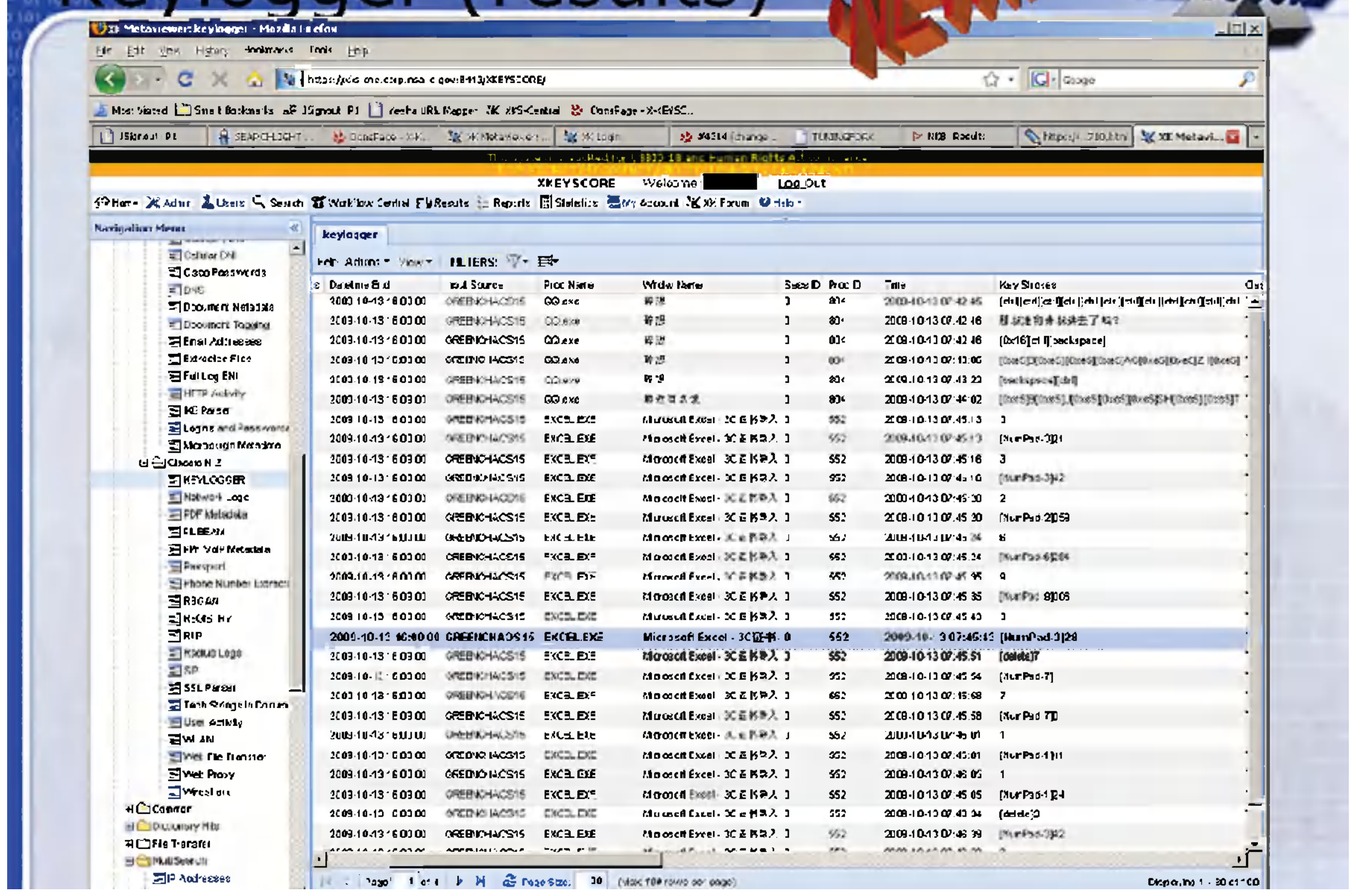
NEW!!

KEYSCORE



Keylogger (results)

NEW!!



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

Keylogger (session viewer)

NEW!

KEYSCORE

XK Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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

Session | Leads (3) | Vets (1)

Formatter: AUTO

Quick Clicks

Session

One-Click Searches

find application

dn:_payload/

find opposite sid

:0 -->

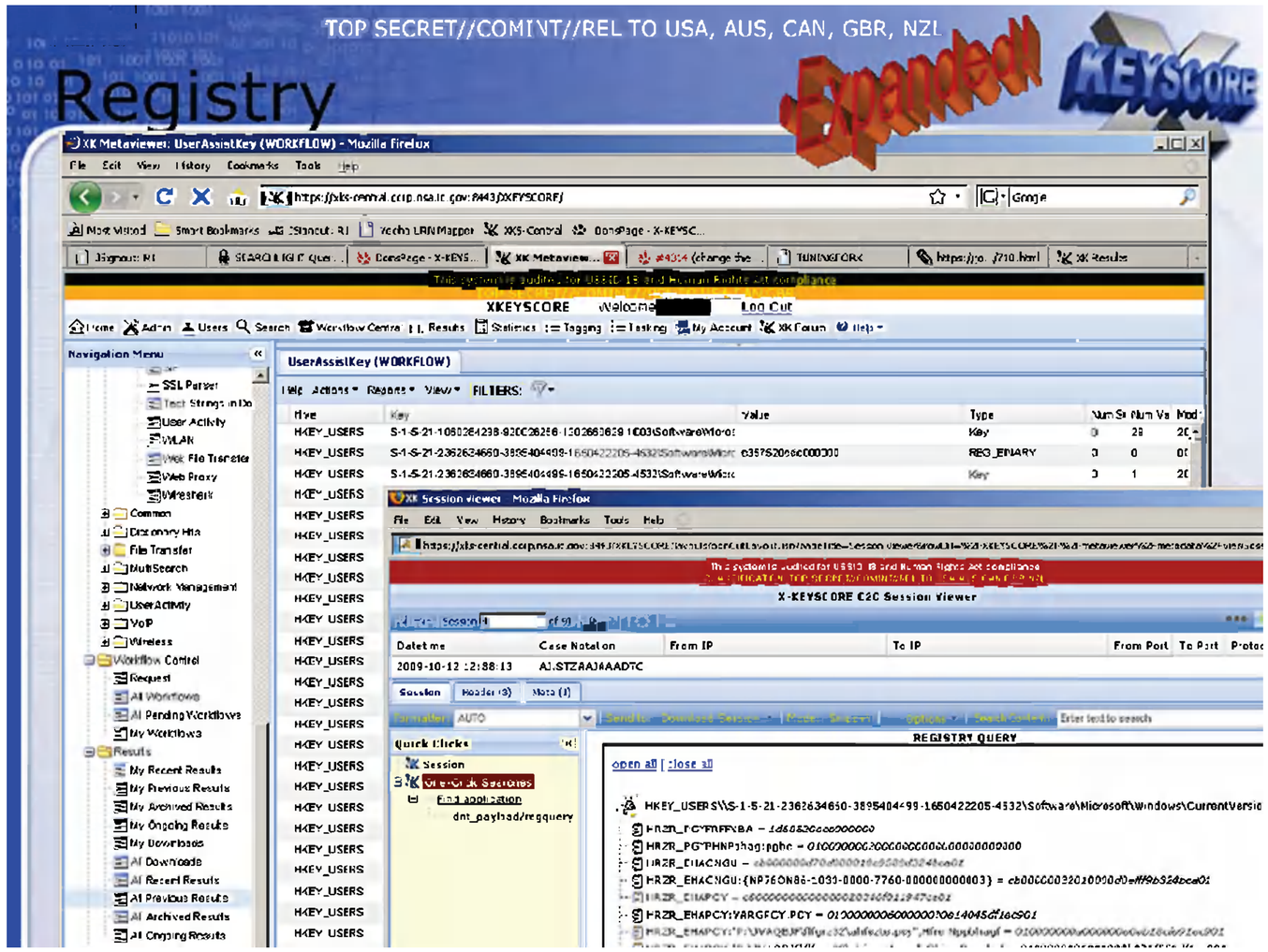
:0

KEYLOGGER

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

Keystroke Legend

	QQ.exe/8040	EXCEL.EXE/5520	MSACCESS.EXE/1580/0	MSACCESS.EXE
Window Title:	聊聊	Microsoft Excel - 3CuF 13号入工作周报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][ts]			
2009-10-13T7:43:6.921	[0xe5]B[0xe5]H[0xe5][0xe5]AO[0xe5] [0xe5]ZH[0xe5]U[0xe5]N[0xe5] [0xe5]HE[0xe5][0xe5] [0xe5]F3[0xe5]I[0xe5]E[0xe5]I[0xe5] [0xe5]AO[0xe5][0xe5][.][0xe5][0xe5] [0xe5]ZJO[0xe5][0xe5]IT[0xe5] [0xe5]AN[0xe5][0xe5][0xe5]DE[0xe5] [0xe5]0[0xe5]2[0xe5][0xe5]YE[0xe5] [0xe5]BU[0xe5][0xe5][0xe5]ZIH[0xe5] [0xe5]D[0xe5]AO[0xe5][0xe5] [0xe5]JI[0xe5]N[0xe5][0xe5]QU[0xe5] [0xe5]NE[0xe5]I[0xe5][0xe5]N3[0xe5] [sd][0xe5][sa][~]			
2009-10-13T7:43:22.15	[ts][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
KEYSCORE
XKEYSCORE
Log Out
UserAssistKey (WORKFLOW)
REGISTRY QUERY

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

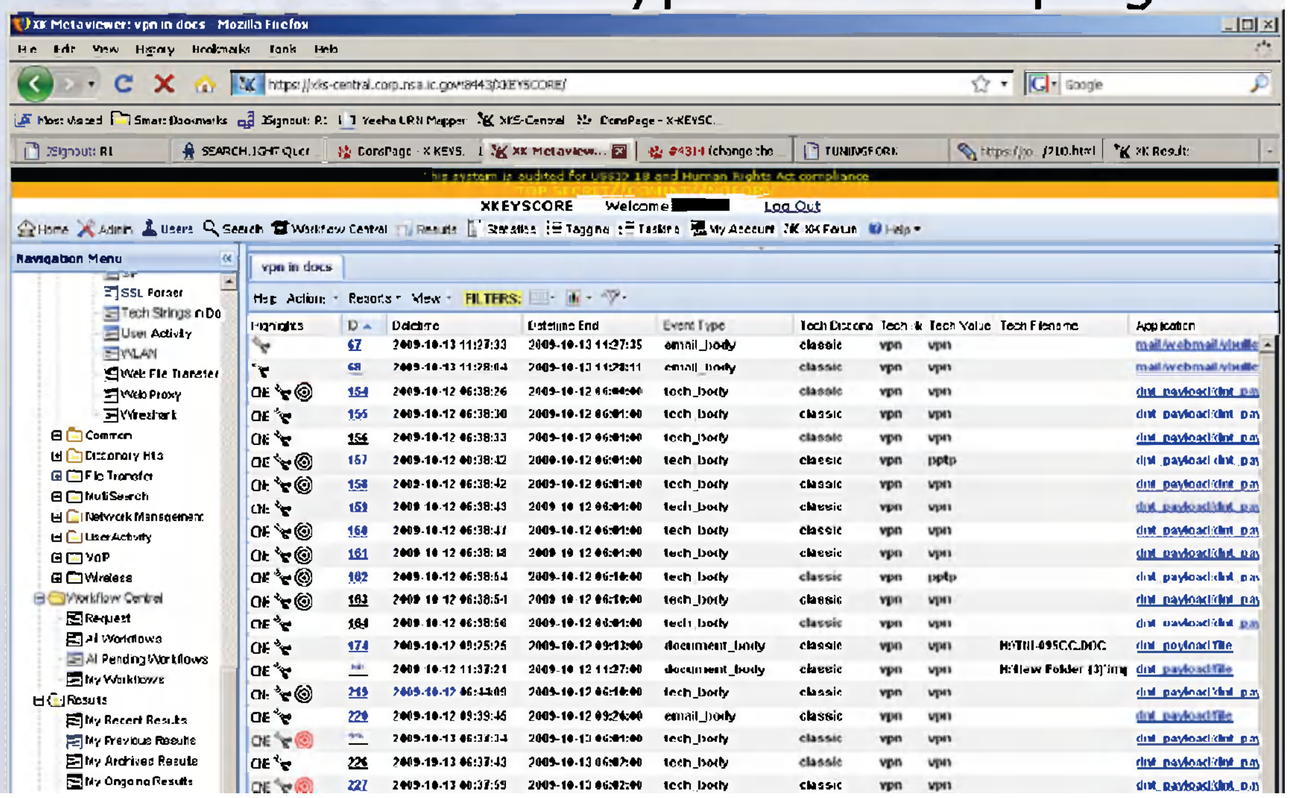
Other Payloads

- 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

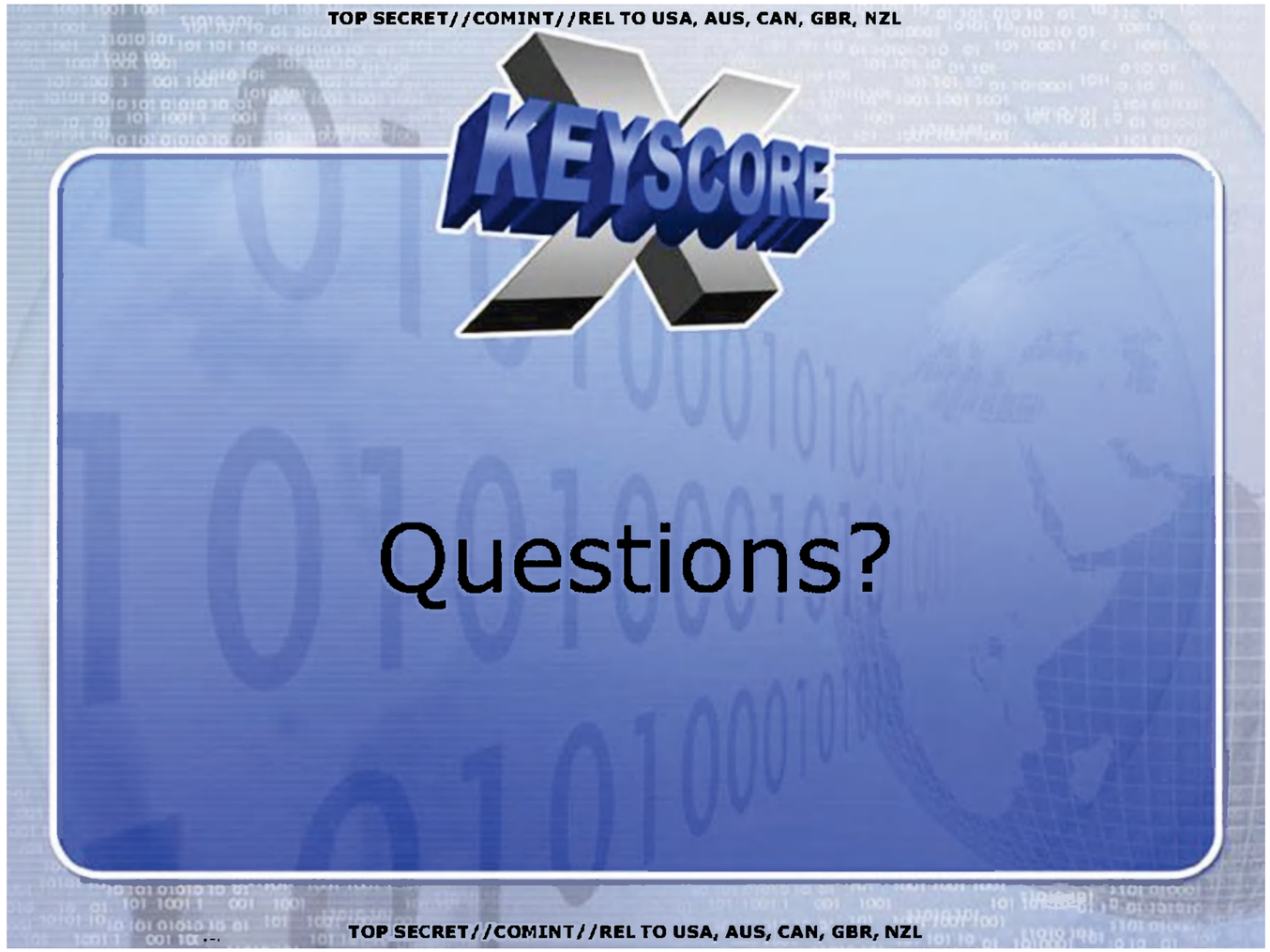
Tech Strings in Documents

- Catchall for data types without plugins



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



Questions?

Blank

- Page