KEYSCORE

XKEYSCORE for Counter-CNE

"Using the XKS CNE dataset and a DISGRUNTLEDDUCK fingerprint, we now see at least 21 TAO boxes with evidence of this intrusion set, most of which are associated with projects aimed at Iran WMD targets." -- **MHS, July 2010**

March, 2011
[redacted]
xks-cne@r1.r.nsa

Overall Classification

The overall classification of this presentation is:

TOP SECRET//COMINT//REL TO USA, FVEY

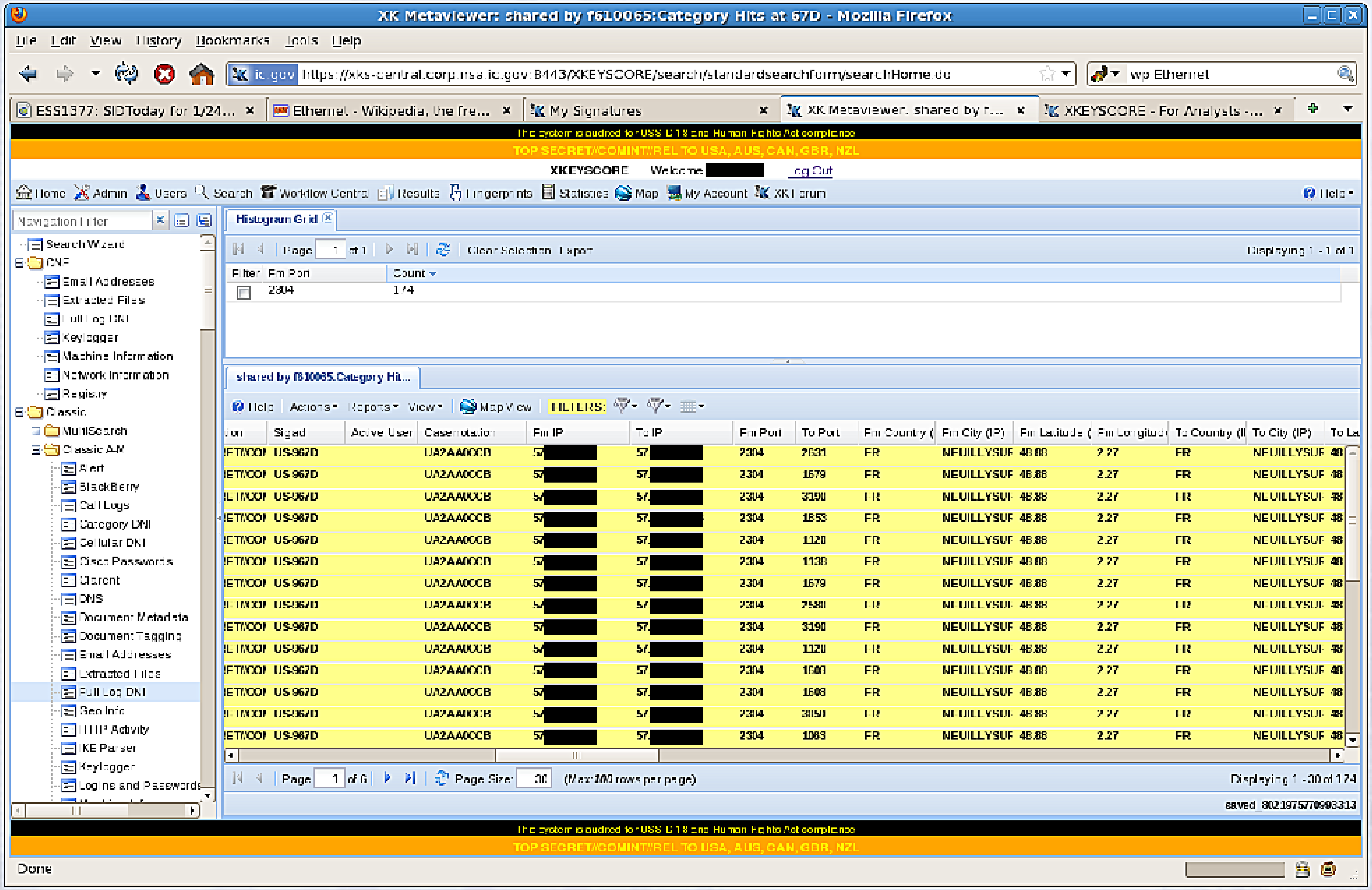
What is XKEYSCORE?

- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
  - Extract and tag metadata & content from traffic
  - Servicing analyst queries and workflows
- Web and programmatic front-ends

What is XKEYSCORE?

- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
  - Extract and tag metadata & content from traffic
  - Servicing analyst queries and workflows
- Web and programmatic front-ends

XKEYSCORE GUI


XK Metaviewer: shared by f610065:Category Hits at 67D - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ic.gov https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/search/standardsearchform/searchHome.do
wp Ethernet
ES51377: SIDToday for 1/24...
Ethernet - Wikipedia, the fre...
My Signatures
XK Metaviewer: shared by f...
XKEYSCORE - For Analysts -...

The 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 Fingerprints Statistics Map My Account XKForum Help
Navigation Filter
Search Wizard
CNE
Email Addresses
Extracted Files
Full Log DNI
Keylogger
Machine Information
Network Information
Registry
Classic
MultiSearch
Classic A/V
Alert
BlackBerry
Call Logs
Category DNI
Cellular DNI
Cisco Passwords
Clarent
DNS
Document Metadata
Document Tagging
Email Addresses
Extracted Files
Full Log DNI
Geo Info
HTTP Activity
IKE Parser
Keylogger
Logins and Passwords
Histogram Grid
Page 1 of 1
Clear Selection Export
Displaying 1 - 1 of 1

Filter	Frm Port	Count
□	2304	174

shared by f610065.Category Hit...
Help Actions Reports View Map View FILTERS:

...ion	Sigad	Active User	Casenotation	Frm IP	To IP	Frm Port	To Port	Frm Country (	Frm City (IP)	Frm Latitude (	Frm Longitude	To Country (I	To City (IP)	To La...
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57 [redacted]	2304	2631	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	1853	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57 [redacted]	2304	1138	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57 [redacted]	2304	7580	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57 [redacted]	2304	1600	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	1608	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57 [redacted]	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48
ETWCOI	US-987D		UA2AA0CCB	57 [redacted]	57. [redacted]	2304	1063	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48

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

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

Example Search

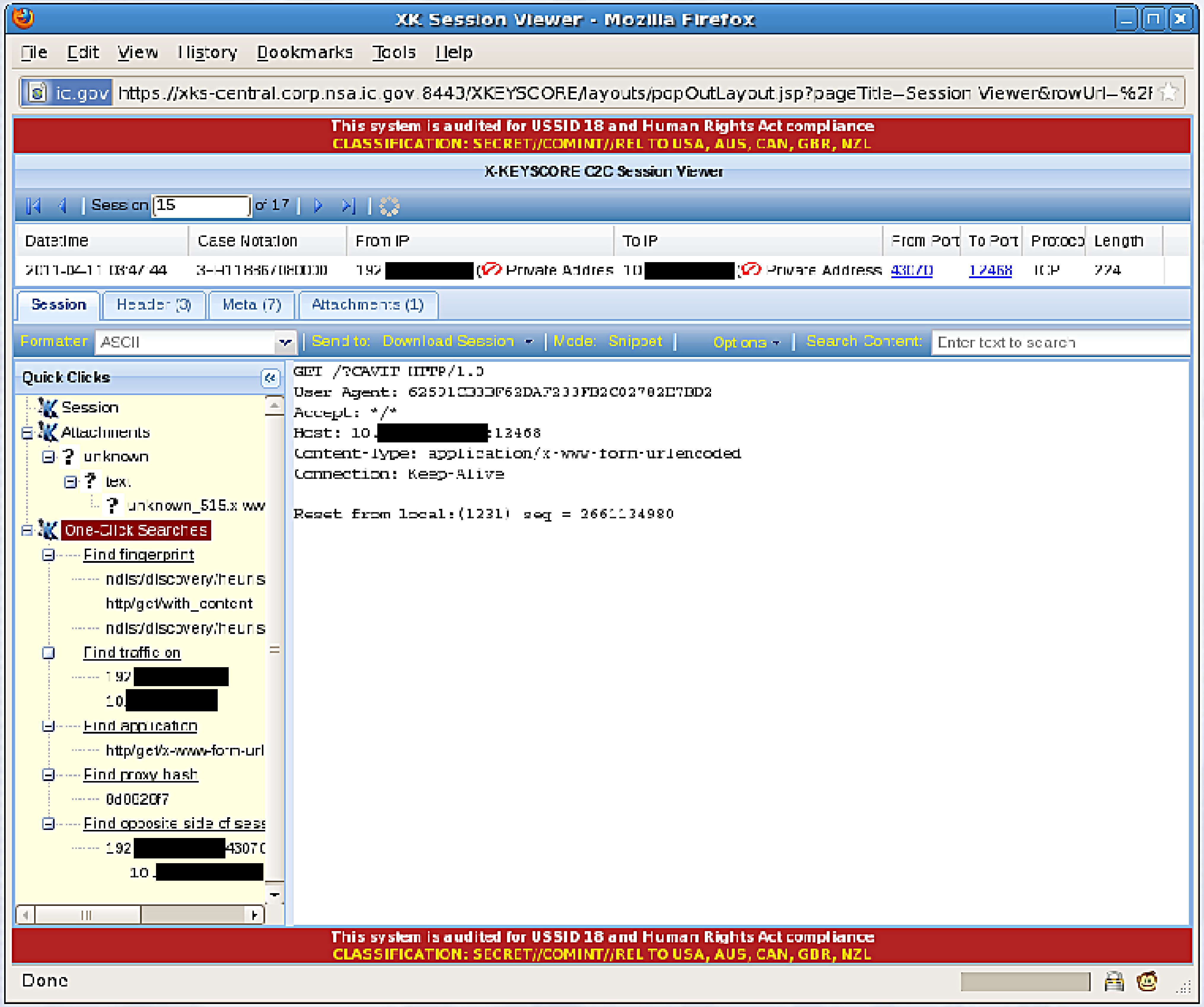
- Let’s try a search for suspicious stuff…

  http_activity search, 5-eyes defeat, look for fingerprints:

  `ndist/discovery/heuristic/BHAM/get_with_content` or `http/get/with_content`

- While the search runs, some gotchas:
  - You choose where your query is run
  - Content and metadata age-off
  - Burden is on user/auditor to comply with USSID-18 or other rules
  - Geolocation based on IP

Search Results


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

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

X-KEYSCORE C2C Session Viewer

Session 15 of 17

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-11 08:47:44	3-4118867080000	192 [redacted] Private Address	10 [redacted] Private Address	43070	12468	TCP	224

192 [redacted]
10 [redacted]

192 [redacted] 43070
10 [redacted]

```
GET /?CAVIT HTTP/1.0
User Agent: 62501C003F62DA7300FD2C02702D7DD2
Accept: */*
Host: 10.[redacted]:12468
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

Reset from local:(1231) seq = 2661134980
```

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

Notes:

- Strange User-Agent
- Probably NOT CNE but definitely something non-standard
- Content: maybe a HTTP tunnel for some weird protocol?

`Reset from local...`

- Should we write a Fingerprint?

Fingerprints and Appids

- Useful for identifying classes of traffic or particular targets (for SIGDEV or collection):

```
mail/webmail/yahoo
browser/cellphone/blackberry
topic/s2B/chinese_missile
```

- appid – a contest, highest scoring appid wins
- fingerprint – many fingerprints per session
- microplugin – a fingerprint or appid that is relatively complex (e.g. extracts and databases metadata)

Fingerprints and Appids (more)

- Written in language called “GENESIS” (go genesis-language):

```
appid('encyclopedia/wikipedia', 2.0) =
   http_host('wikipedia' or 'wikimedia‘);
fingerprint('dns/malware/MalwareDomains') =
   dns_host(' erofreex.info ' or ' datayakoz.info '
   or ' erogirlx.info ' or ' pornero.info ' or ...
```

- If a fingerprint contains a `schema` definition, a search form automatically appears in the XKEYSCORE GUI
- Power users can drop in to C++ to express themselves

More about searches

- Many different searches
  - Base search is **Full Log DNI**
  - Depending on traffic type, will generate searchable results for (example):

HTTP Activity	Network Information	GEO Info
Extracted Files	Email Addresses	Registry
Logins and Passwords	Document Metadata	Machine Info

- workflow – a user query that is run automatically usually every 24 hours

XKEYSCORE Gotchas

- Not all sites run latest XKEYSCORE software or fingerprints
- fingerprint submission:
  - XKEYSCORE team weighs mission-worthiness of user fingerprints vs computational cost
- Content and metadata ageoff

XKEYSCORE CNE

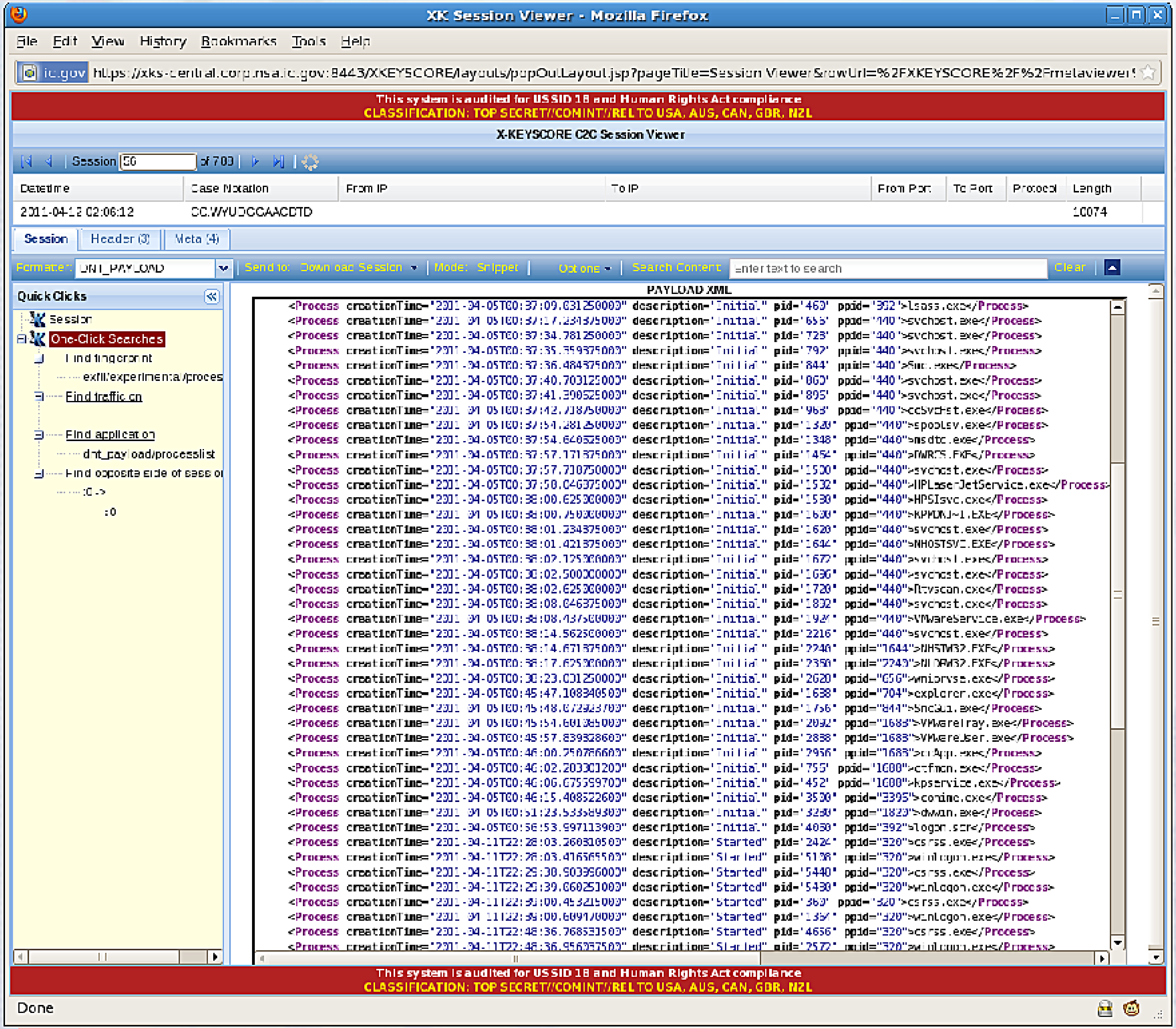
- Lots of endpoint data flows into XKS
  TAO (no ECIs), GCHQ (almost all)
- Other limited flows include SIGINT Forensics Center, TAO STAT
- XKEYSCORE works well for endpoint data
- Sometimes the paradigm breaks (e.g. collected browser history file)

XKEYSCORE CNE (more)

- Payload types:
  `dirwalk, extracted file, system survey, network config, captured credentials, registry query, key logger, etc.`
- Labeled `dnt_payload` in appid/fingerprint ontology
- Let’s look at some DANDERSPRITZ data…

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE (more)


XK Session Viewer - Mozilla Firefox
File Edit View History Bookmarks Tools Help
ic.gov https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaviewer
Session 50 of 703
Session
Header (3)
Meta (4)
Send to: Download Session
Mode: Snippet
Options
Search Content
enter text to search
Clear
Quick Clicks
Done

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

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-12 02:06:12	CC.WYUDCCAACDTD						10074

Formatter: DNT_PAYLOAD

- Session
- One-Click Searches
  - Find fingerprint
    - exfil/experimental/proces
  - Find traffic on
  - Find application
    - dnt_payload/processlist
  - Find opposite side of sess o
    - :0 ->
      :0

PAYLOAD XML

```
<Process creationTime="2011-04-05T00:37:09.031250000" description="Initial" pid='460' ppid='392'>lsass.exe</Process>
<Process creationTime="2011-04-05T00:37:17.234375000" description="Initial" pid='656' ppid='440'>svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:34.781250000" description="Initial" pid='728' ppid='440'>svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:35.359375000" description="Initial" pid='792' ppid='440'>svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:36.484375000" description="Initial" pid='844' ppid='440'>Smc.exe</Process>
<Process creationTime="2011-04-05T00:37:40.703125000" description="Initial" pid='860' ppid='440'>svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:41.390625000" description="Initial" pid='896' ppid='440'>svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:42.718750000" description="Initial" pid='968' ppid='440'>ccSvcHst.exe</Process>
<Process creationTime="2011-04-05T00:37:54.281250000" description="Initial" pid='1320' ppid="440">spoolsv.exe</Process>
<Process creationTime="2011-04-05T00:37:54.640625000" description="Initial" pid='1348' ppid="440">msdtc.exe</Process>
<Process creationTime="2011-04-05T00:37:57.171875000" description="Initial" pid='1454' ppid="440">DWRCS.EXE</Process>
<Process creationTime="2011-04-05T00:37:57.718750000" description="Initial" pid='1500' ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:58.046875000" description="Initial" pid='1532' ppid="440">HPLaserJetService.exe</Process>
<Process creationTime="2011-04-05T00:38:00.625000000" description="Initial" pid='1580' ppid="440">HPSIsvc.exe</Process>
<Process creationTime="2011-04-05T00:38:00.750000000" description="Initial" pid='1600' ppid="440">KPMDKJ~1.EXE</Process>
<Process creationTime="2011-04-05T00:38:01.234375000" description="Initial" pid='1620' ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:01.421875000" description="Initial" pid='1644' ppid="440">NHOSTSVC.EXE</Process>
<Process creationTime="2011-04-05T00:38:02.125000000" description="Initial" pid='1672' ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.500000000" description="Initial" pid='1696' ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.625000000" description="Initial" pid='1720' ppid="440">Rtvscan.exe</Process>
<Process creationTime="2011-04-05T00:38:08.046875000" description="Initial" pid='1832' ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:08.437500000" description="Initial" pid='1924' ppid="440">VMwareService.exe</Process>
<Process creationTime="2011-04-05T00:38:14.562500000" description="Initial" pid='2216' ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:14.671875000" description="Initial" pid='2240' ppid="1644">NHSTW32.EXE</Process>
<Process creationTime="2011-04-05T00:38:17.625000000" description="Initial" pid='2350' ppid="2240">NLDRW32.EXE</Process>
<Process creationTime="2011-04-05T00:38:23.031250000" description="Initial" pid='2620' ppid="656">wmiprvse.exe</Process>
<Process creationTime="2011-04-05T00:45:47.108340500" description="Initial" pid='1688' ppid="704">explorer.exe</Process>
<Process creationTime="2011-04-05T00:45:48.672923700" description="Initial" pid='1756' ppid="844">SmcGui.exe</Process>
<Process creationTime="2011-04-05T00:45:54.601365000" description="Initial" pid='2092' ppid="1688">VMwareTray.exe</Process>
<Process creationTime="2011-04-05T00:45:57.839328600" description="Initial" pid='2888' ppid="1688">VMwareUser.exe</Process>
<Process creationTime="2011-04-05T00:46:00.750786600" description="Initial" pid='2956' ppid="1688">ccApp.exe</Process>
<Process creationTime="2011-04-05T00:46:02.203301200" description="Initial" pid='755' ppid='1600'>ctfmon.exe</Process>
<Process creationTime="2011-04-05T00:46:06.675359700" description="Initial" pid='452' ppid='1600'>kpservice.exe</Process>
<Process creationTime="2011-04-05T00:46:15.408522600" description="Initial" pid='3500' ppid="3396">conime.exe</Process>
<Process creationTime="2011-04-05T00:51:23.533589300" description="Initial" pid='3280' ppid="1820">dwwin.exe</Process>
<Process creationTime="2011-04-05T00:56:53.997113900" description="Initial" pid='4080' ppid="392">logon.scr</Process>
<Process creationTime="2011-04-11T22:28:03.260810500" description="Started" pid='2424' ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:28:03.416365500" description="Started" pid='5108' ppid="320">winlogon.exe</Process>
<Process creationTime="2011-04-11T22:29:30.903396000" description="Started" pid='5440' ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:29:39.060250000" description="Started" pid='5480' ppid="320">winlogon.exe</Process>
<Process creationTime="2011-04-11T22:39:00.453215000" description="Started" pid='360' ppid='320'>csrss.exe</Process>
<Process creationTime="2011-04-11T22:39:00.609170000" description="Started" pid='1357' ppid="320">winlogon.exe</Process>
<Process creationTime="2011-04-11T22:48:36.768531500" description="Started" pid='4656' ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:48:36.956957500" description="Started" pid='2572' ppid="320">winlogon.exe</Process>
```

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

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE (more)

- Recent Developments
  - Upgrade of XKEYSCORE CNE
  - Keyloggers: keylogger/perfect/extension
  - PCAP Reingestion
- Router Redirection

Counter CNE Methodology

(refer to Counter CNE Resources slide...)

- Hypothesis/research-driven
  - “Could South Korean CNE be using similar selectors to FVEY CNE?”
  - “What keywords could be used to find keyloggers (“example: keylog OR keystroke”)
- Bogus or Unusual Traffic
  - HTTP GET with content (example in this presentation)
  - HTTP POST at odd hours (from Russia 0200-0359Z)
  - Funky user agents
- Known-Host or User driven (e.g. drop sites)
- XKEYSCORE is GOOD at these kinds of things

CNE-Specific

- Registry searches (e.g. SIMBAR)
- Fused Active/Passive search
  - common selectors
  - document hashes
- Known Processes (malicious executables or code)

  … Let's enhance the process list appid
- map-reduce within CNE cluster using GENESIS calls

XKEYSCORE Doesn't Do...

- ... at all (well, automatically, anyways)
  - Paired traffic heuristic-based approach
    - HTTP[S] imbalance (e.g. GET without response)
    - IP/DNS mismatch*
- ... on an automatic basis
  - Network or host characterization
  - Changes in IP/DNS mapping over time
  - Changes over time in malware comms

Counter CNE Resources

- *How to Discover Intrusions [using XKEYSCORE]* by [redacted] and [redacted] (paper)
- MHS INDEX – Foreign CNE Discovery Page

  https://wiki.itd.nsa/wiki/Foreign_CNE_Discovery
- CSEC and GCHQ – DONUT (unknown protocols):

  https://tiso.sigint.cse/snipehunt/index.php/DONUT
- GCHQ Discovery Posted some Research of Detecting Man-on-the-Side Attacks:

  https://tiso.sigint.cse/snipehunt/index.php/MOTS

GCQH Disco Team posts POC's for different Intrusions and some Details:

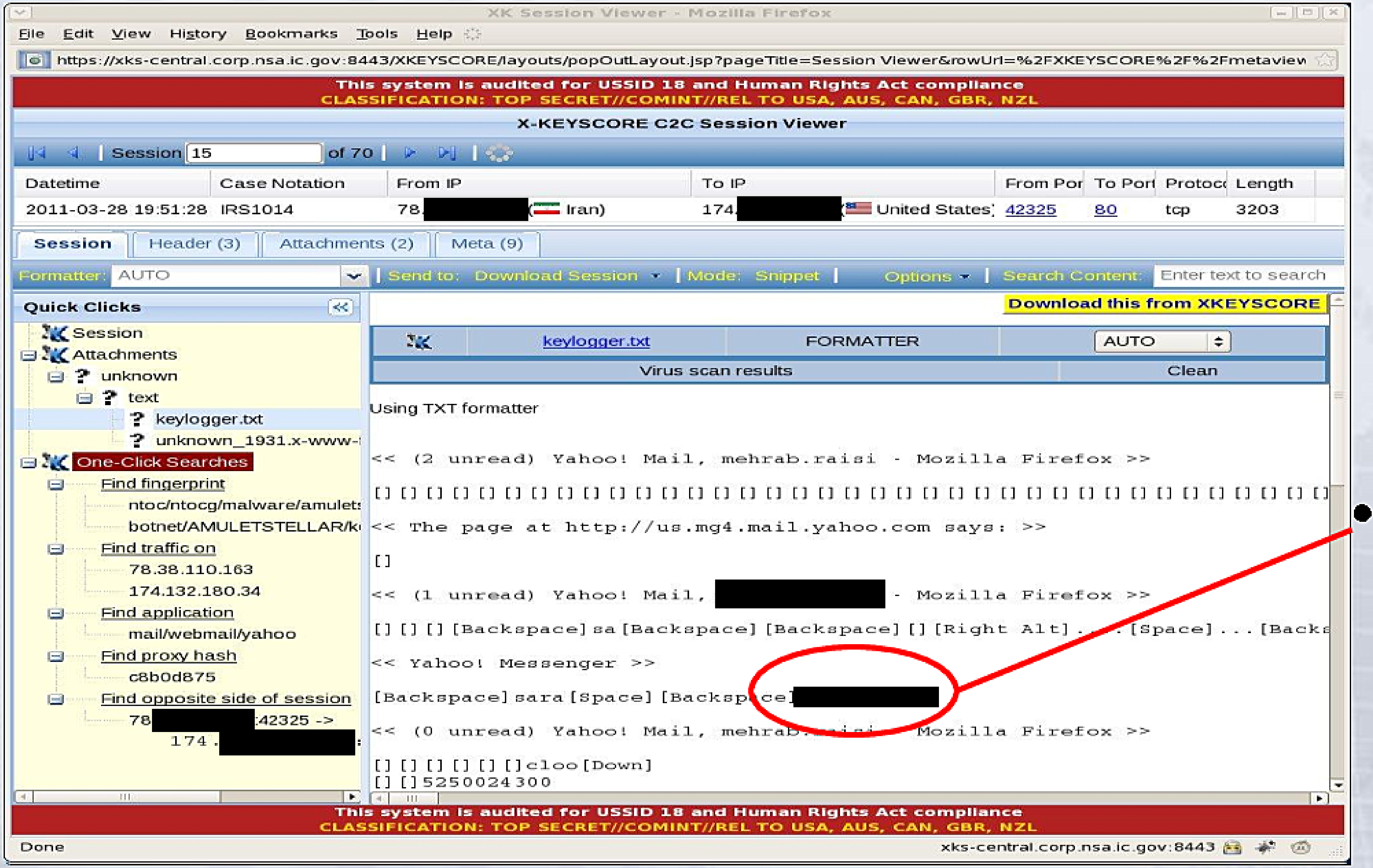
  https://wiki.gchq/index.php/Discovery

- The GCHQ DISCO team also posts Discovery Theories they run once a week:

  https://wiki.gchq/index.php/Discovery_Afternoons
- XKEYSCORE Fingerprints

Success Story – MHS INDEX

Using TAO-obtained Iranian implant encryption keys, inline decrypt using XKS microplugin – IRGC-QF keylogger data!



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%2Fmetaview

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 15 of 70

Datetime	Case Notation	From IP	To IP	From Por	To Port	Protoco	Length
2011-03-28 19:51:28	IRS1014	78.[redacted](Iran)	174.[redacted](United States)	42325	80	tcp	3203

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

Quick Clicks

- Session
- Attachments
  - unknown
    - text
      - keylogger.txt
      - unknown_1931.x-www-
- One-Click Searches
  - Find fingerprint
    - ntoc/ntocg/malware/amulets
    - botnet/AMULETSTELLAR/k
  - Find traffic on
    - 78.38.110.163
    - 174.132.180.34
  - Find application
    - mail/webmail/yahoo
  - Find proxy hash
    - c8b0d875
  - Find opposite side of session
    - 78[redacted]:42325 ->
    - 174.[redacted]

Download this from XKEYSCORE

	keylogger.txt	FORMATTER	AUTO
Virus scan results			Clean

Using TXT formatter

```
<< (2 unread) Yahoo! Mail, mehrab.raisi - Mozilla Firefox >>

[][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][][]

<< The page at http://us.mg4.mail.yahoo.com says: >>

[]

<< (1 unread) Yahoo! Mail, [redacted] - Mozilla Firefox >>

[][][][Backspace]sa[Backspace][Backspace][][Right Alt]....[Space]...[Backs

<< Yahoo! Messenger >>

[Backspace]sara[Space][Backspace][redacted]

<< (0 unread) Yahoo! Mail, mehrab.raisi - Mozilla Firefox >>

[][][][][][]cloo[Down]
[][]5250024300
```

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

Done   xks-central.corp.nsa.ic.gov:8443

- Login

Points of Contact

- MHS Index Team
  [redacted]: [redacted]@nsa.ic.gov
- CES/TRANGRESSION
  [redacted]: [redacted]@nsa.ic.gov
  [redacted]: [redacted]@nsa.ic.gov
- NSA/Countering Foreign Intelligence
  [redacted]: [redacted]@nsa.ic.gov
- NTOC ??
- XKEYSCORE
  [redacted], [redacted]: xks-cne@r1.r.nsa