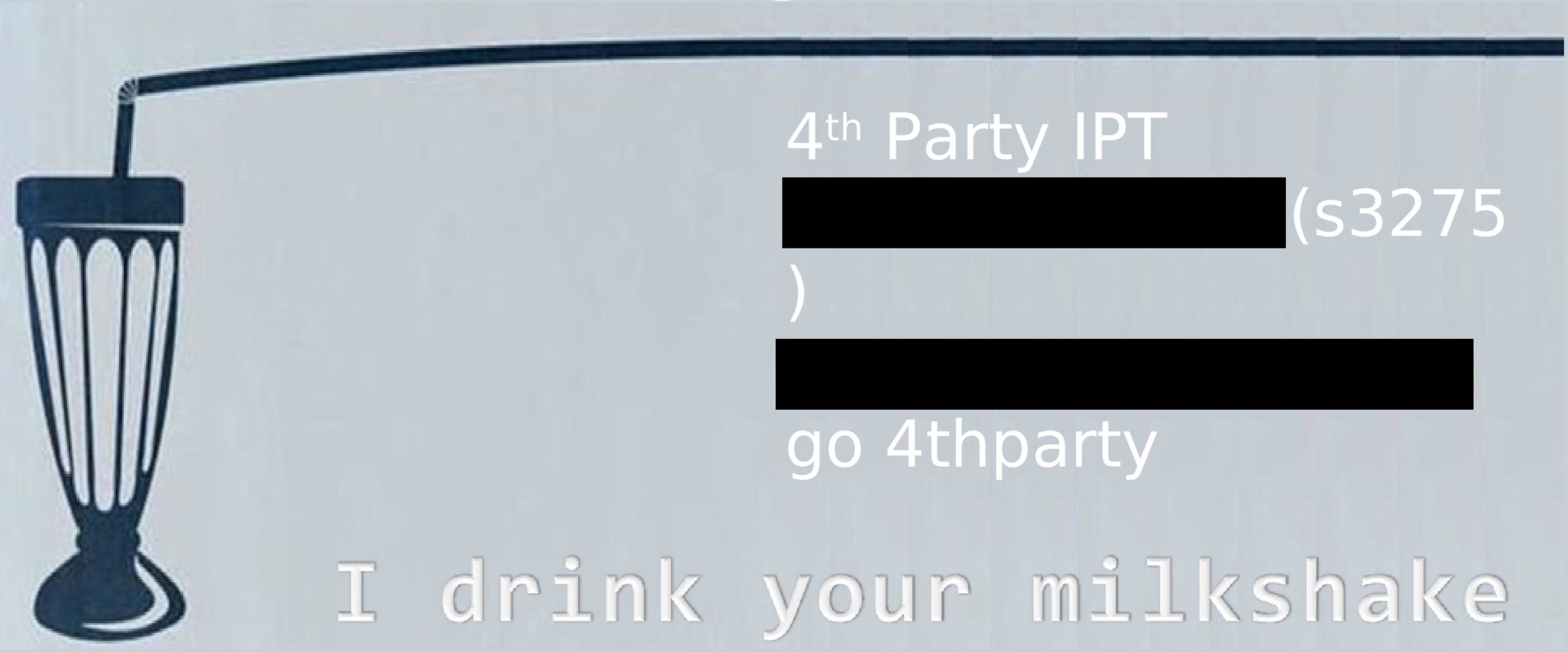
(U) Fourth Party Opportunities



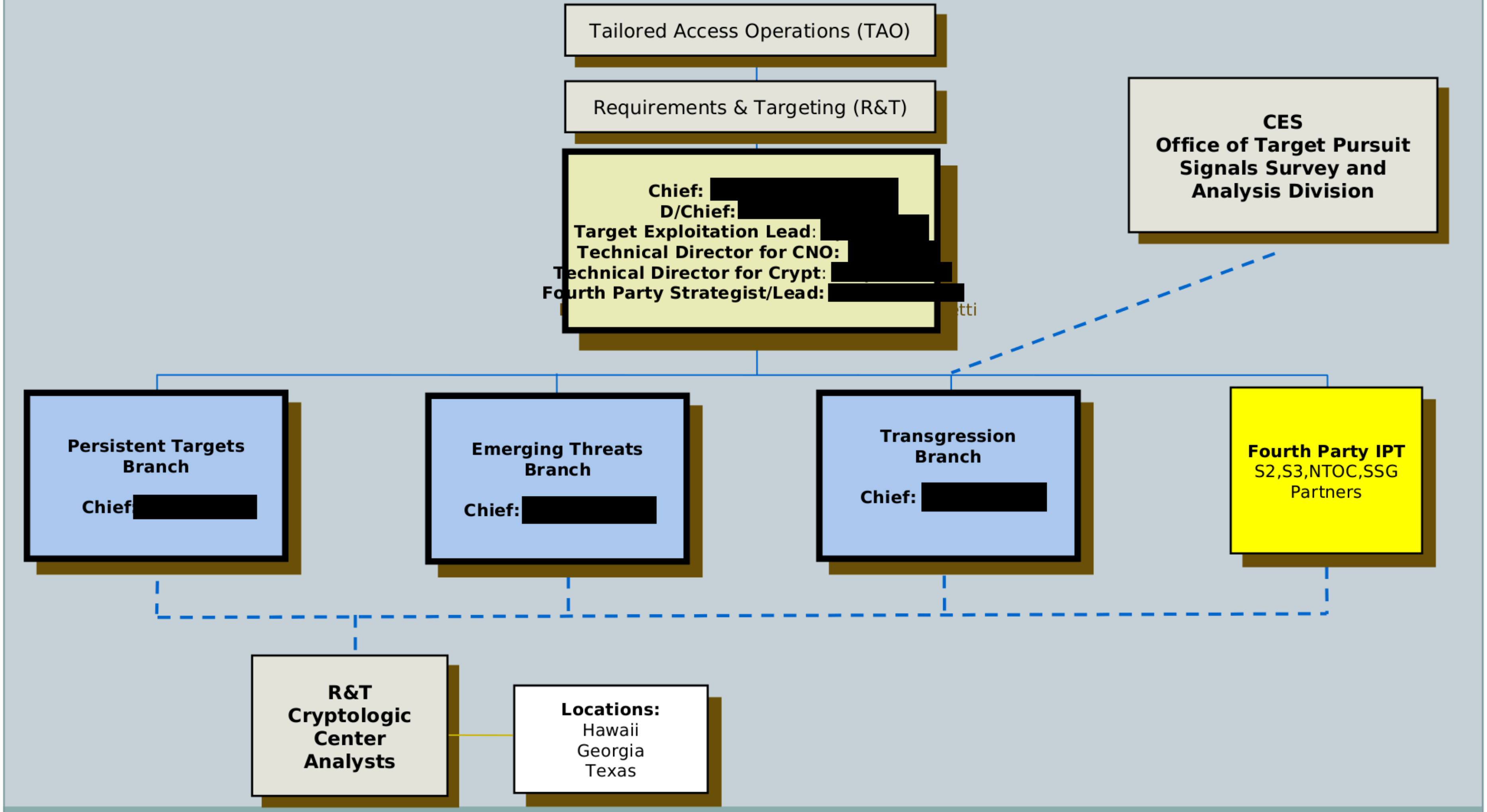
4th Party IPT

[redacted] (s3275)

[redacted]

go 4thparty

(U//FOUO) Cyber Counterintelligence Division



Tailored Access Operations (TAO)

Requirements & Targeting (R&T)

Chief: [redacted]
D/Chief: [redacted]
Target Exploitation Lead: [redacted]
Technical Director for CNO: [redacted]
Technical Director for Crypt: [redacted]
Fourth Party Strategist/Lead: [redacted]

CES
Office of Target Pursuit
Signals Survey and
Analysis Division

Persistent Targets Branch

Chief [redacted]

Emerging Threats Branch

Chief: [redacted]

Transgression Branch

Chief: [redacted]

Fourth Party IPT
S2,S3,NTOC,SSG
Partners

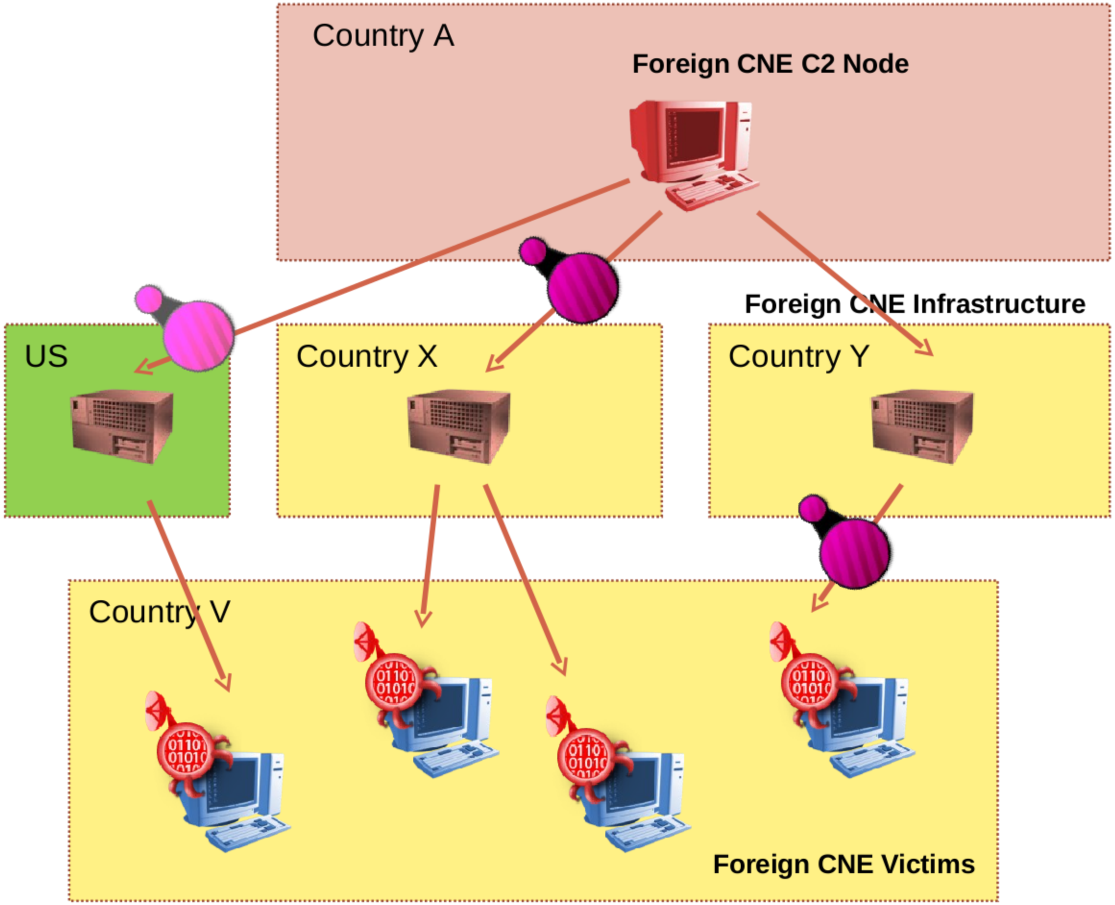
R&T Cryptologic Center Analysts

Locations:
Hawaii
Georgia
Texas

(U) What is 4th Party

- (S//SI//REL) 4th party collection leverages CCNE accesses to provide Foreign Intelligence from foreign CNE victims
- (U) Types of 4th Party opportunities
  - (U) Passive Acquisition
  - (U) Active Acquisition
  - (U) Victim Stealing / Sharing
  - (U) Re-purposing

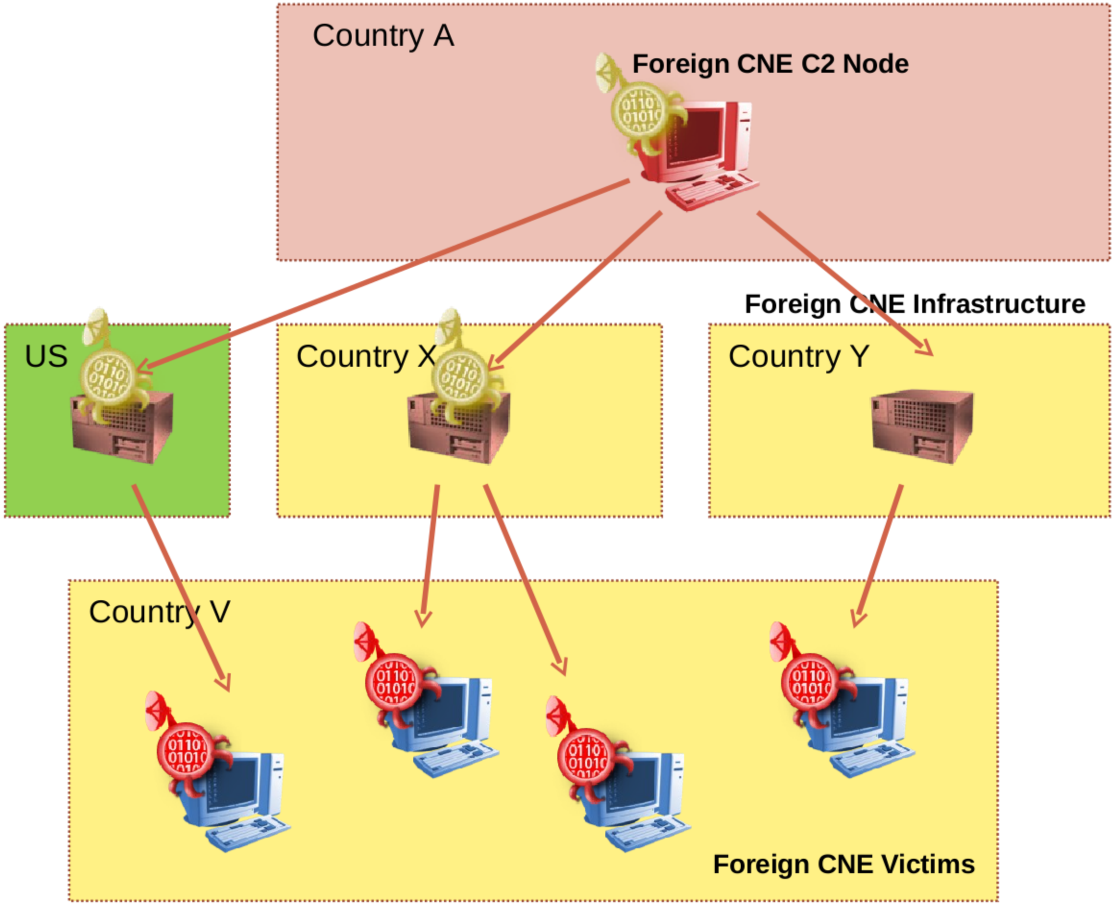
(S//SI//REL) *Passive acquisition* utilizes mid-point collection to target information being ex-filtrated from victims of foreign CNE activities. This often involves CES efforts to decrypt or de-obfuscate the collected data.



S//SI//REL

(U) Passive Acquisition

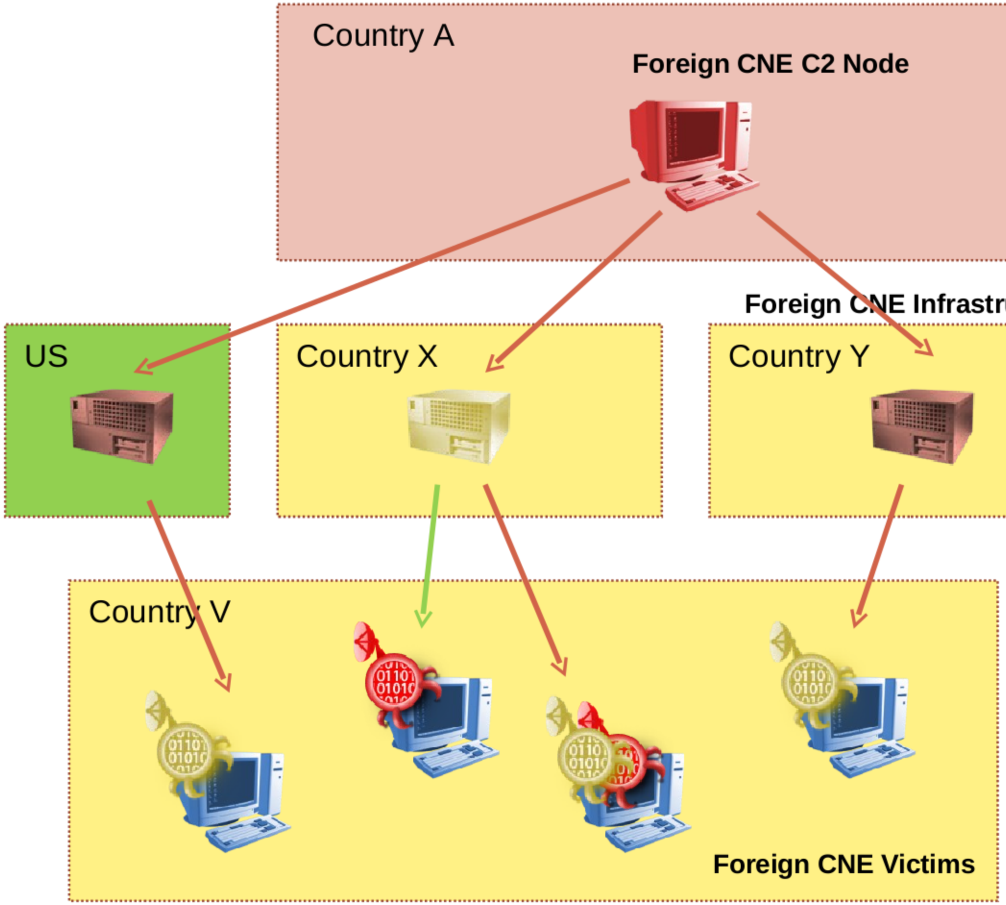
(S//SI//REL) *Active acquisition* utilizes end-point collection to target foreign CNE infrastructure in order to collect victim information.



S//SI//REL

(U) Active Acquisition

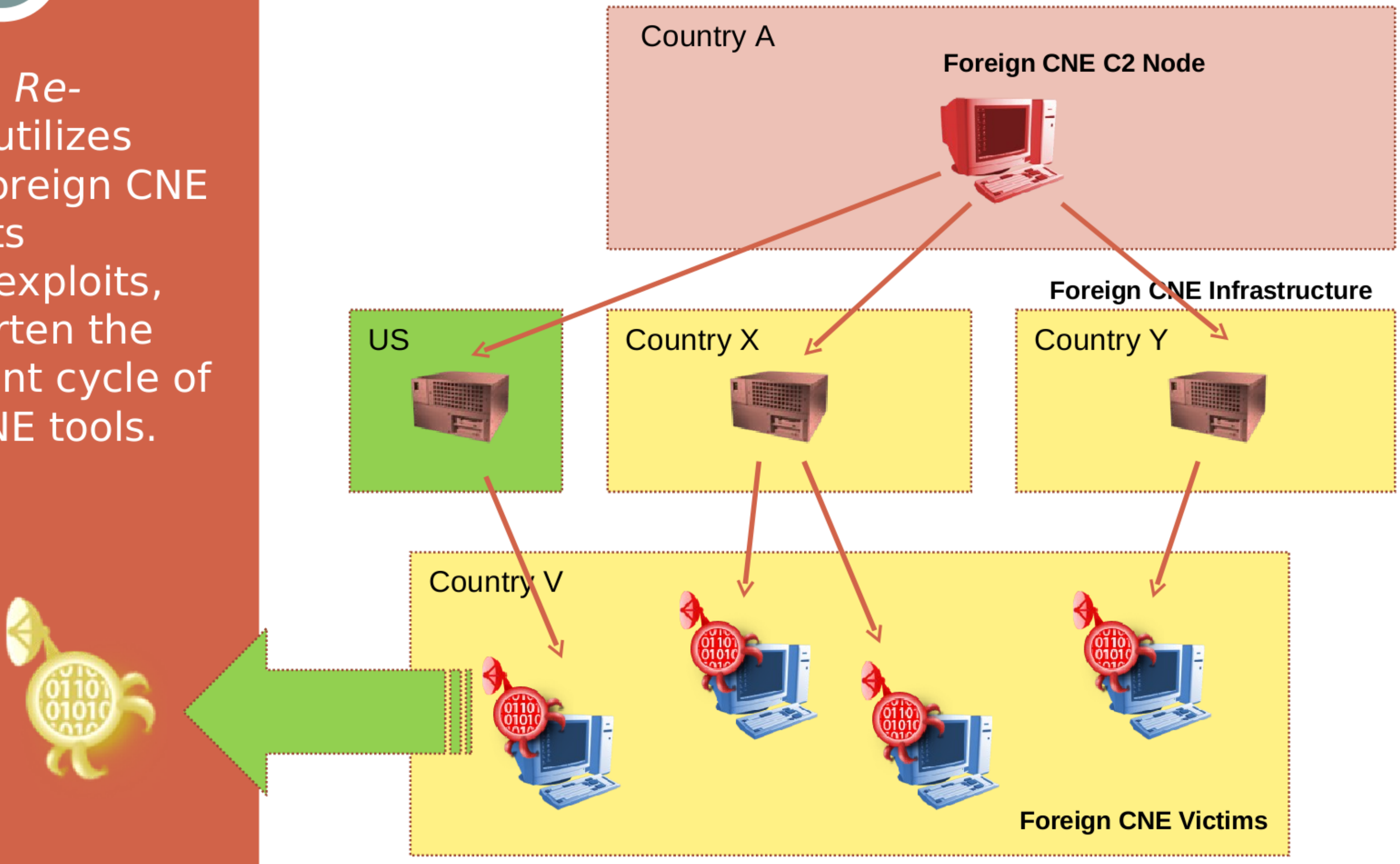
(S//SI//REL) *Victim stealing* exploits weaknesses in foreign CNE implants and C2 systems to gain access to victims and either take control of the foreign implant or replace it with our own. This is NOT a disruption or CNA activity. It is solely used to further CNE accesses.



S//SI//REL

(U) Victim Stealing / Sharing

(S//SI//REL) *Re-purposing* utilizes captured foreign CNE components (implants, exploits, etc) to shorten the development cycle of our own CNE tools.

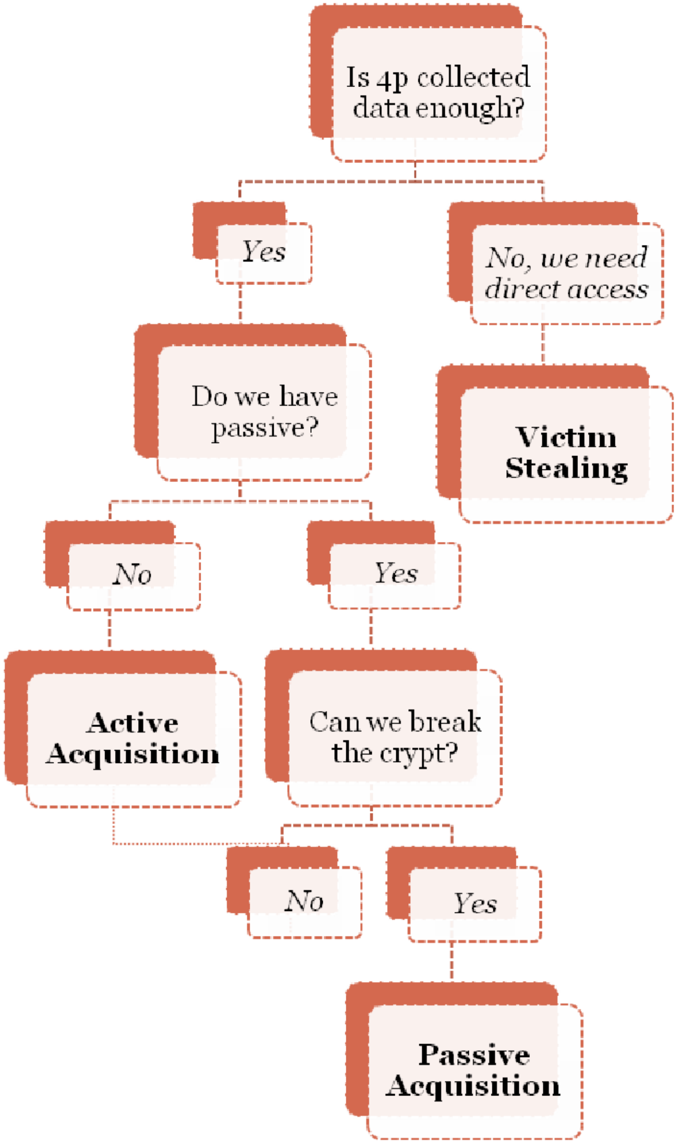


S//SI//REL

(U) Re-purposing

(U) 4th Party Decision Tree

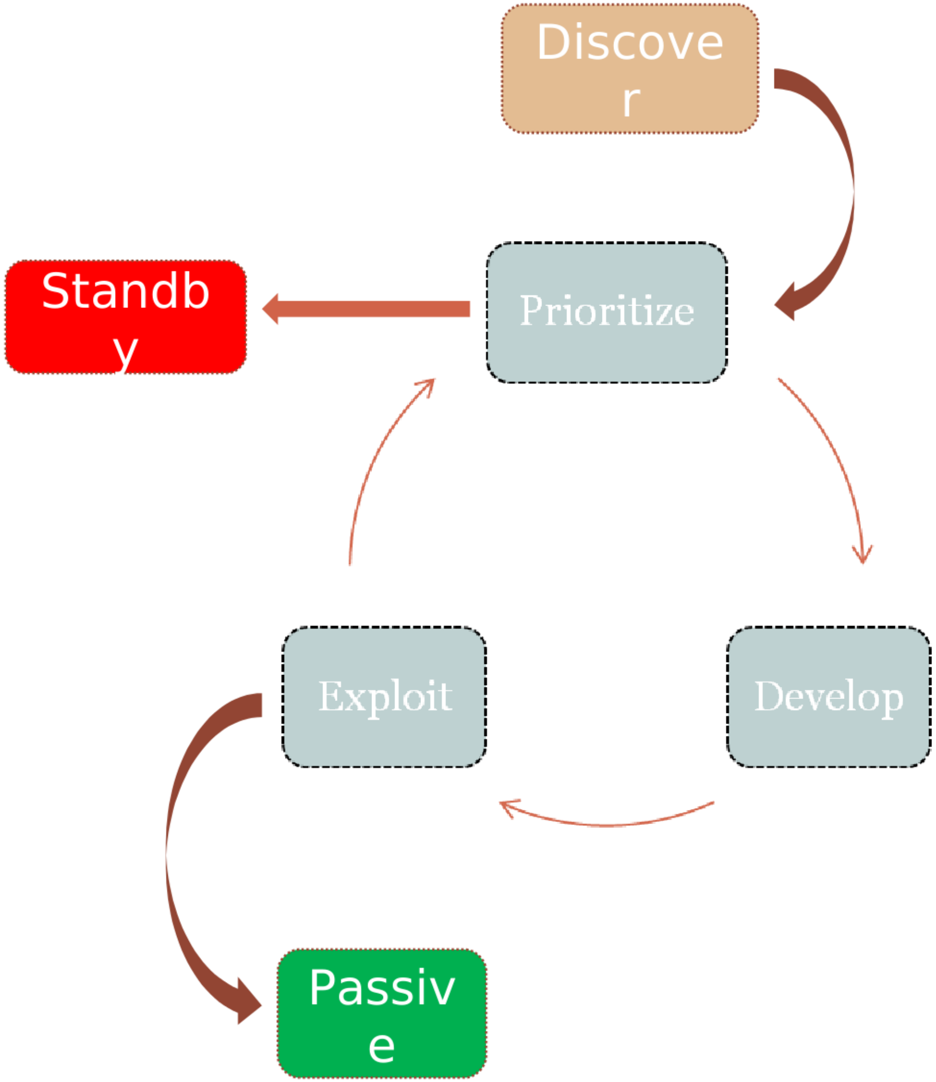
(S//REL) The best sustained outcome is *passive acquisition* of valuable 4th party collected information. Where the 4th party is not collecting information of interest, but the victim is still of interest *victim stealing* can be pursued. Where passive or cryptographic issues prevent (or delay) passive acquisition, *active acquisition* will be pursued.



S//SI//REL

(U) 4th Party Lifecycle

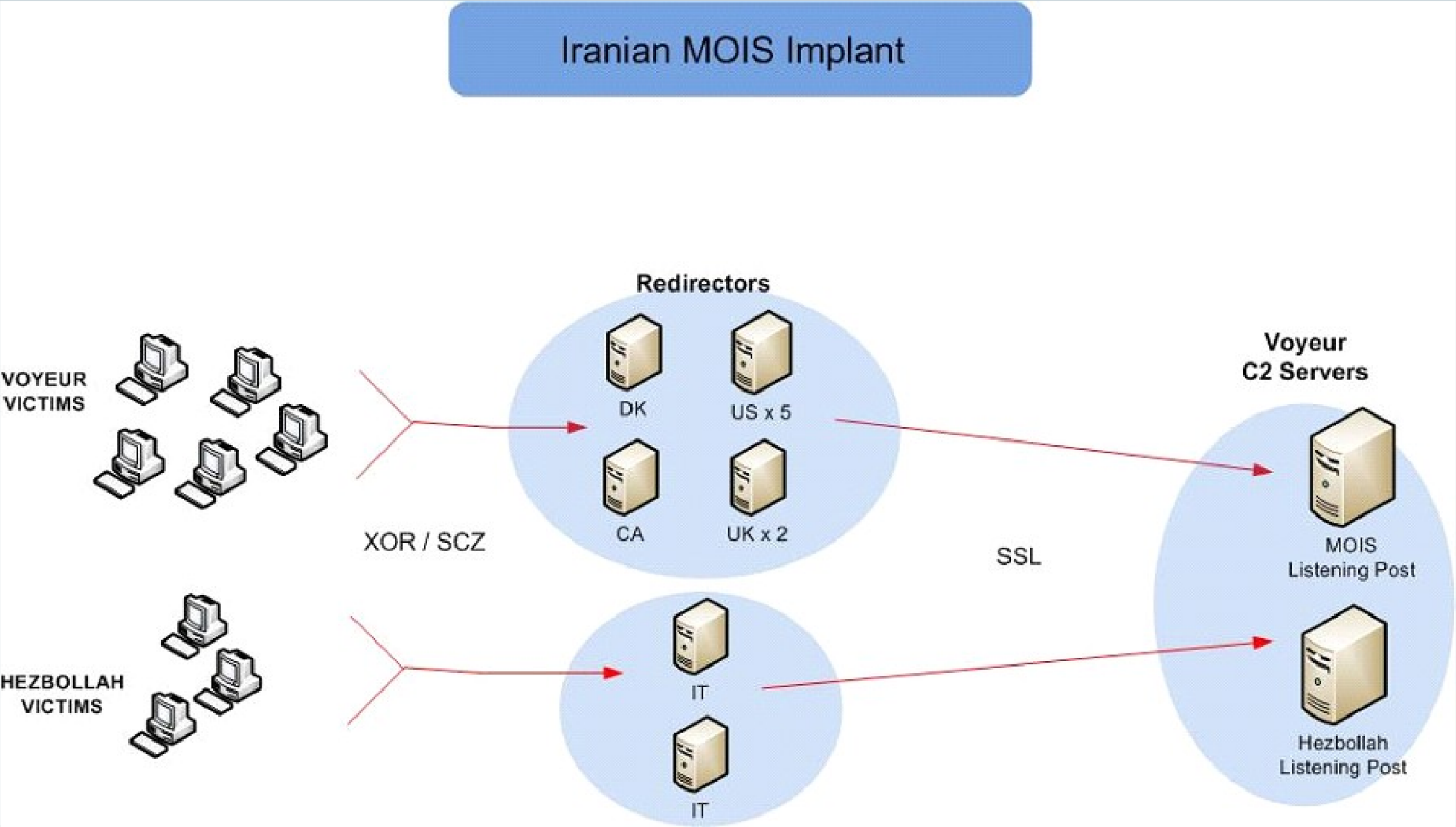
(S//REL) The prioritization, development and exploitation cycle is continuous until the priority is lowered to standby or the intelligence value is being realized through passive alone.



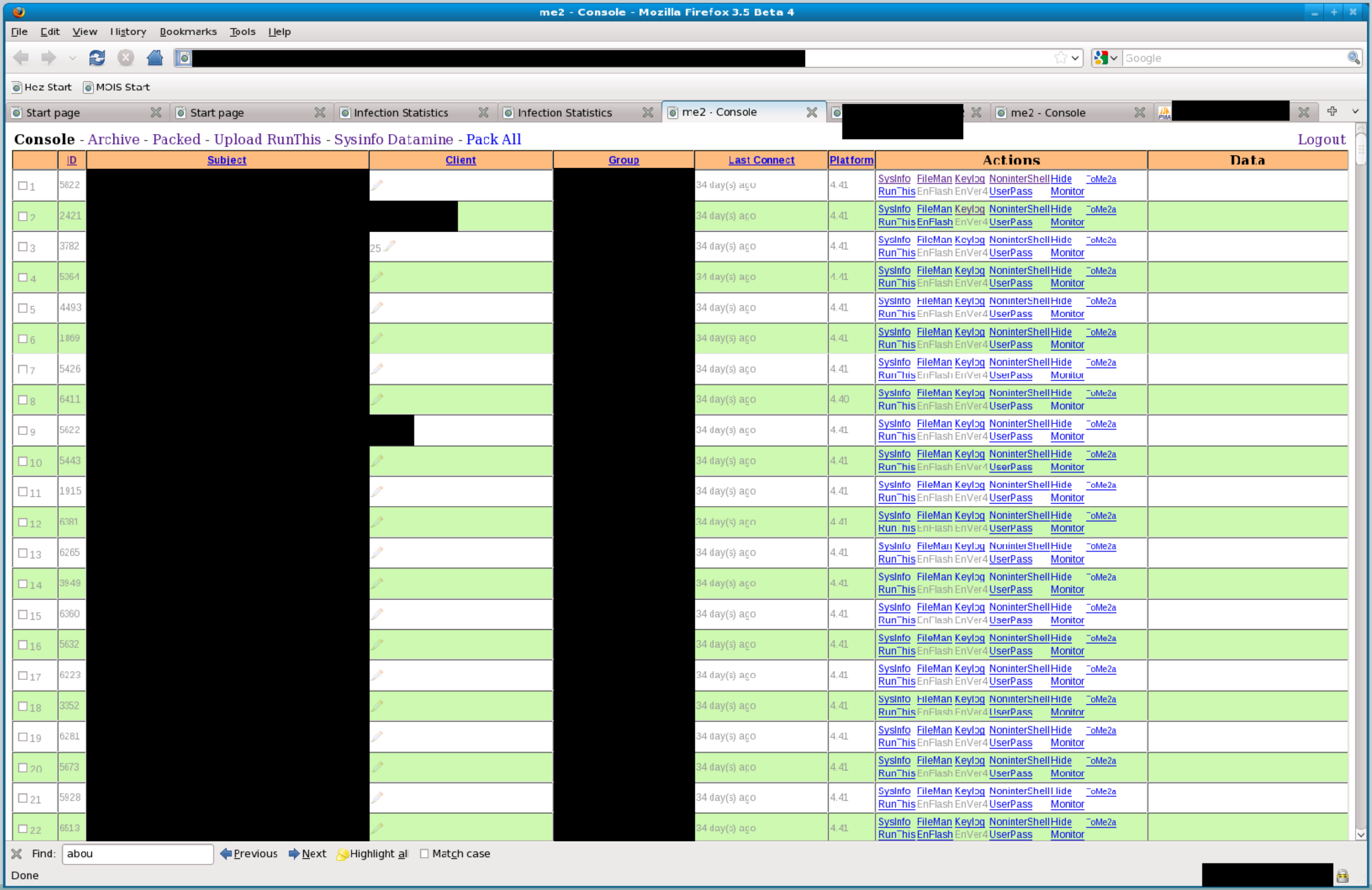
Fourth Party Example

VOYEUR

(U) VOYEUR Network Map



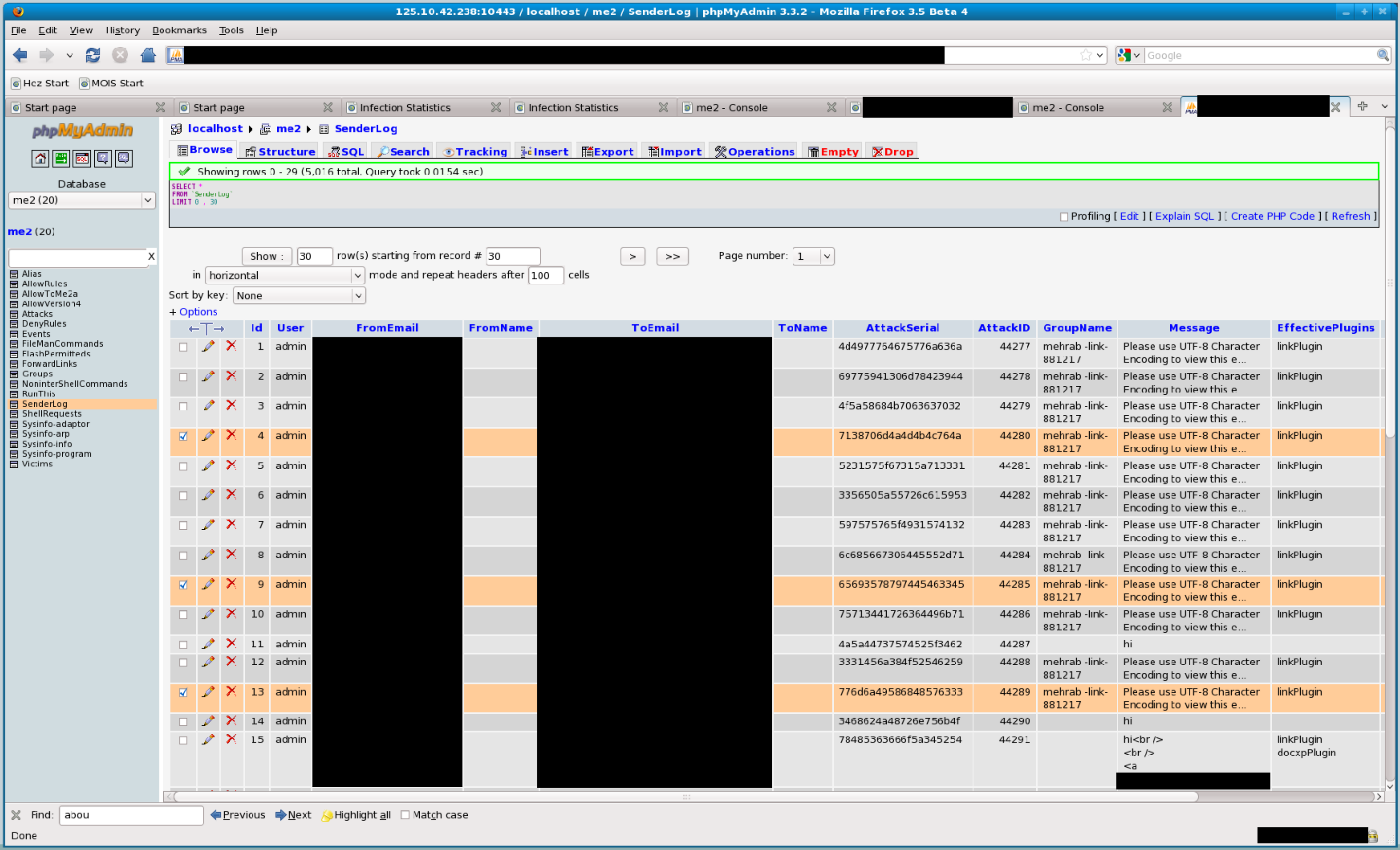
(U) VOYEUR Backend



Console - Archive - Packed - Upload RunThis - Sysinfo Datamine - Pack All   Logout

	ID	Subject	Client	Group	Last Connect	Platform	Actions	Data
□ 1	5822	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 2	2421	[redacted]	[redacted]	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 3	3782	[redacted]	25 ✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 4	5364	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 5	4493	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 6	1869	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 7	5426	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 8	6411	[redacted]	✎	[redacted]	34 day(s) ago	4.40	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 9	5622	[redacted]	[redacted]	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 10	5443	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 11	1915	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 12	6381	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 13	6265	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 14	3949	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 15	6360	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 16	5632	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 17	6223	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 18	3352	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 19	6281	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 20	5673	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 21	5928	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	
□ 22	6513	[redacted]	✎	[redacted]	34 day(s) ago	4.41	SysInfo FileMan Keylog NoninterShell Hide ToMe2a RunThis EnFlash EnVer4 UserPass Monitor	

(U) VOYEUR SQL Interface



Database: me2 (20)

me2 (20)

- Alias
- AllowRules
- AllowToMe2a
- AllowVersion4
- Attacks
- DenyRules
- Events
- FileManCommands
- FlashPermitteds
- ForwardLinks
- Groups
- NoninterShellCommands
- RunThis
- SenderLog
- ShellRequests
- Sysinfo-adaptor
- Sysinfo-arp
- Sysinfo-info
- Sysinfo-program
- Victims

localhost ▸ me2 ▸ SenderLog

Browse | Structure | SQL | Search | Tracking | Insert | Export | Import | Operations | Empty | Drop

✓ Showing rows 0 - 29 (5,016 total, Query took 0.0154 sec)

```
SELECT *
FROM `SenderLog`
LIMIT 0 , 30
```

□ Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]

Show : 30 row(s) starting from record # 30 > >> Page number: 1

in horizontal mode and repeat headers after 100 cells

Sort by key: None

+ Options

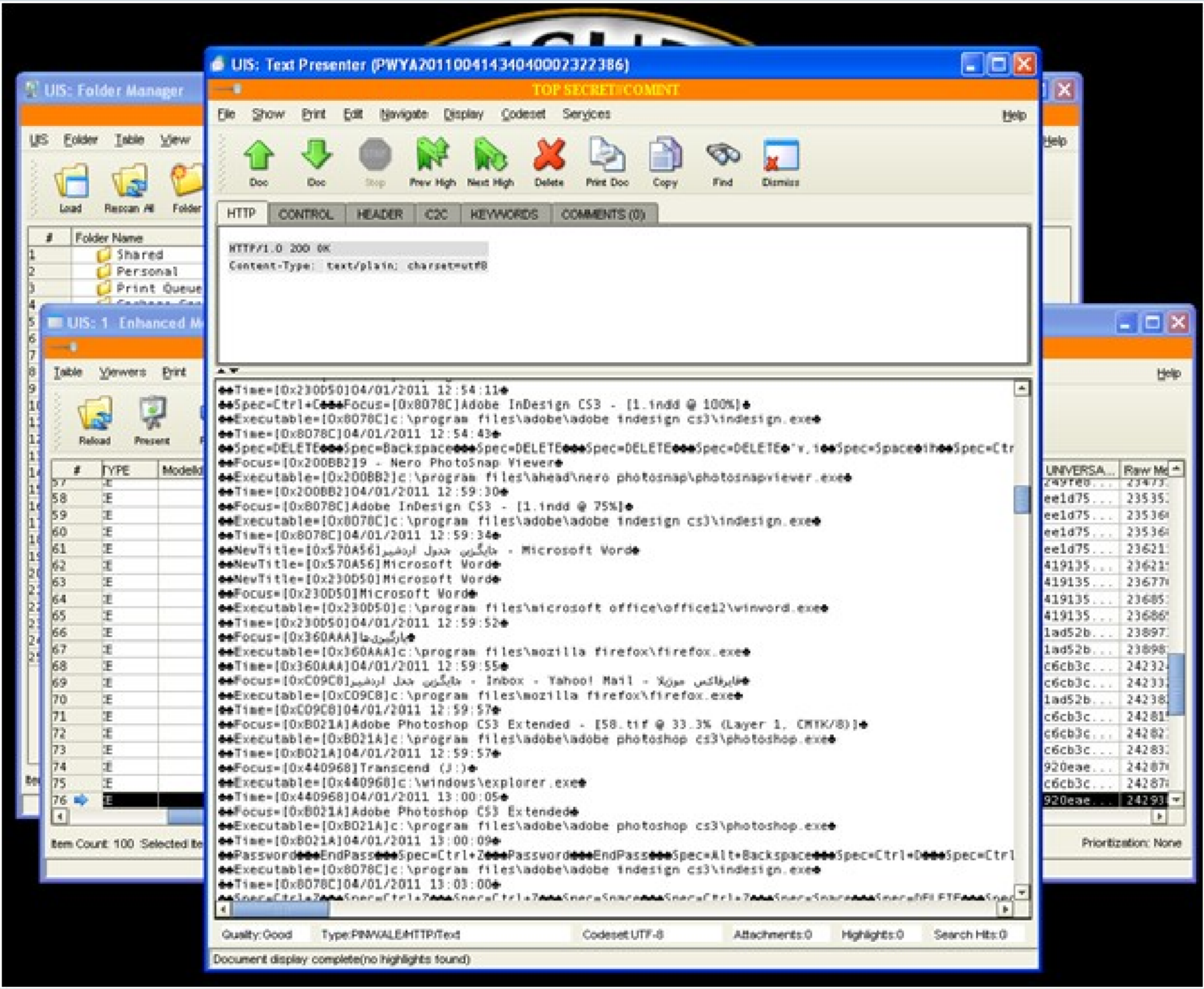
←T→			Id	User	FromEmail	FromName	ToEmail	ToName	AttackSerial	AttackID	GroupName	Message	EffectivePlugins
☐	✎	✗	1	admin	[redacted]		[redacted]		4d4977754675776a636a	44277	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	2	admin	[redacted]		[redacted]		69775941306d78423944	44278	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	3	admin	[redacted]		[redacted]		4f5a58684b7063637032	44279	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☑	✎	✗	4	admin	[redacted]		[redacted]		7138706d4a4d4b4c764a	44280	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	5	admin	[redacted]		[redacted]		5231575f67315a713331	44281	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	6	admin	[redacted]		[redacted]		3356505a55726c615953	44282	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	7	admin	[redacted]		[redacted]		597575765f4931574132	44283	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	8	admin	[redacted]		[redacted]		6c685667306445552d71	44284	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☑	✎	✗	9	admin	[redacted]		[redacted]		65693578797445463345	44285	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	10	admin	[redacted]		[redacted]		75713441726364496b71	44286	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	11	admin	[redacted]		[redacted]		4a5a44737574525f3462	44287		hi	
☐	✎	✗	12	admin	[redacted]		[redacted]		3331456a384f52546259	44288	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☑	✎	✗	13	admin	[redacted]		[redacted]		776d6a49586848576333	44289	mehrab -link-881217	Please use UTF-8 Character Encoding to view this e...	linkPlugin
☐	✎	✗	14	admin	[redacted]		[redacted]		3468624a48726e756b4f	44290		hi	
☐	✎	✗	15	admin	[redacted]		[redacted]		78485363666f5a345254	44291		hi<br /> <br /> <a [redacted]	linkPlugin docxpPlugin

Find: abou Previous Next Highlight all □ Match case

Done

[redacted]

(U) UIS


UIS: Text Presenter (PWYA20110041434040002322386)
TOP SECRET//COMINT
File Show Print Edit Navigate Display Codeset Services Help
Doc Doc Stop Prev High Next High Delete Print Doc Copy Find Dismiss
HTTP CONTROL HEADER C2C KEYWORDS COMMENTS (0)
UIS: Folder Manager
UIS Folder Table View
Load Rescan All Folder
# Folder Name
Shared
Personal
Print Queue
UIS: 1 Enhanced M
Table Viewers Print
Reload Present
# TYPE Modeld
Item Count: 100 Selected Ite
UNIVERSA... Raw Me
Prioritization: None

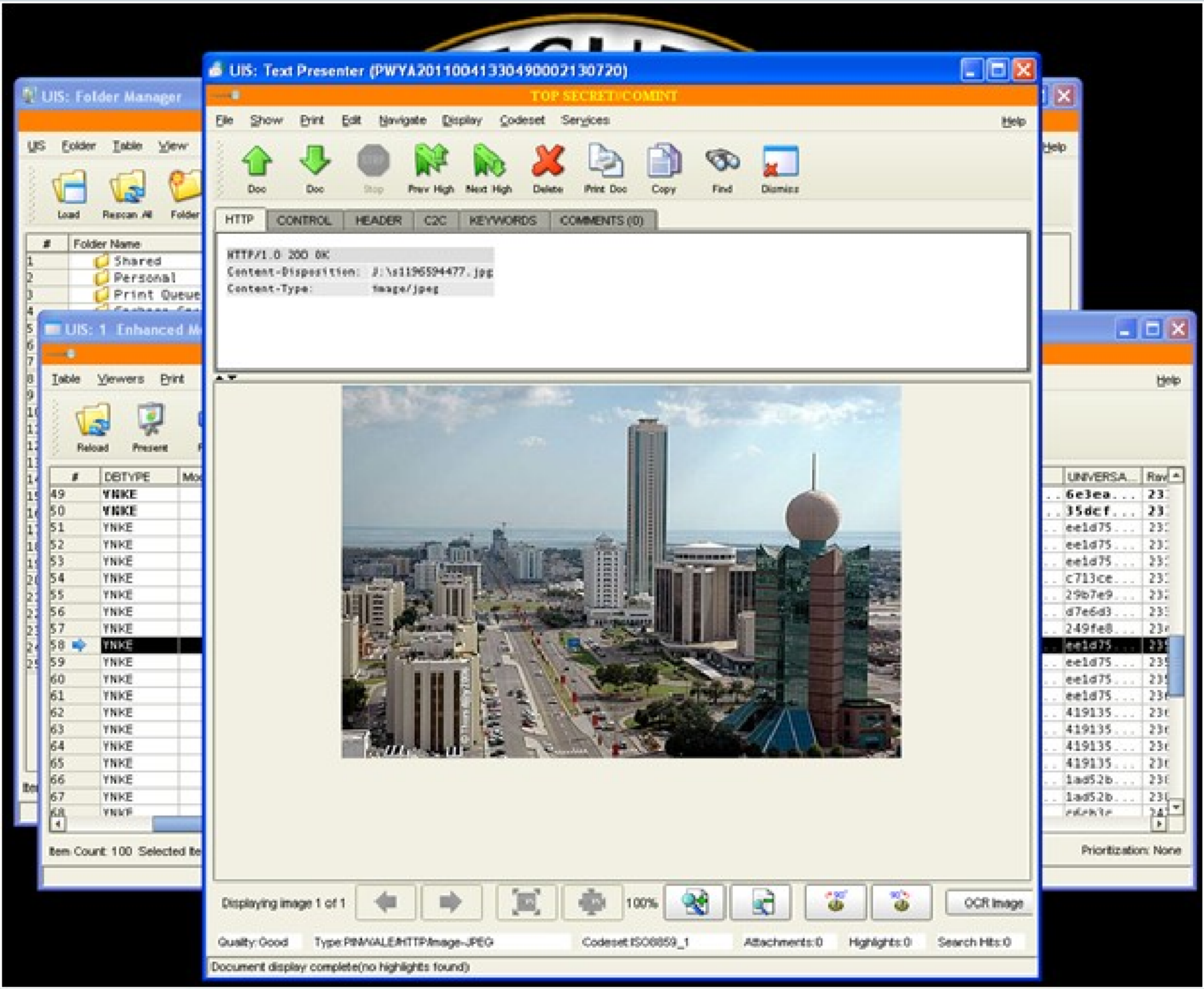
```
HTTP/1.0 200 OK
Content-Type: text/plain; charset=utf8
```

```
◆◆Time=[0x230D50]04/01/2011 12:54:11◆
◆◆Spec=Ctrl+C◆◆◆Focus=[0x8078C]Adobe InDesign CS3 - [1.indd @ 100%]◆
◆◆Executable=[0x8078C]c:\program files\adobe\adobe indesign cs3\indesign.exe◆
◆◆Time=[0x8078C]04/01/2011 12:54:43◆
◆◆Spec=DELETE◆◆◆Spec=Backspace◆◆◆Spec=DELETE◆◆◆Spec=DELETE◆◆◆Spec=DELETE◆"v,i◆◆Spec=Space◆ih◆◆Spec=Ctr
◆◆Focus=[0x200BB2]19 - Nero PhotoSnap Viewer◆
◆◆Executable=[0x200BB2]c:\program files\ahead\nero photosnap\photosnapviewer.exe◆
◆◆Time=[0x200BB2]04/01/2011 12:59:30◆
◆◆Focus=[0x8078C]Adobe InDesign CS3 - [1.indd @ 75%]◆
◆◆Executable=[0x8078C]c:\program files\adobe\adobe indesign cs3\indesign.exe◆
◆◆Time=[0x8078C]04/01/2011 12:59:34◆
◆◆NewTitle=[0x570A56]بایگانی جدول اردشیر - Microsoft Word◆
◆◆NewTitle=[0x570A56]Microsoft Word◆
◆◆NewTitle=[0x230D50]Microsoft Word◆
◆◆Focus=[0x230D50]Microsoft Word◆
◆◆Executable=[0x230D50]c:\program files\microsoft office\office12\winword.exe◆
◆◆Time=[0x230D50]04/01/2011 12:59:52◆
◆◆Focus=[0x360AAA]بارگیری‌ها◆
◆◆Executable=[0x360AAA]c:\program files\mozilla firefox\firefox.exe◆
◆◆Time=[0x360AAA]04/01/2011 12:59:55◆
◆◆Focus=[0xC09C8]بایگانی جدول اردشیر - Inbox - Yahoo! Mail - موزیلا فایرفاکس◆
◆◆Executable=[0xC09C8]c:\program files\mozilla firefox\firefox.exe◆
◆◆Time=[0xC09C8]04/01/2011 12:59:57◆
◆◆Focus=[0xB021A]Adobe Photoshop CS3 Extended - [58.tif @ 33.3% (Layer 1, CMYK/8)]◆
◆◆Executable=[0xB021A]c:\program files\adobe\adobe photoshop cs3\photoshop.exe◆
◆◆Time=[0xB021A]04/01/2011 12:59:57◆
◆◆Focus=[0x440968]Transcend (J:)◆
◆◆Executable=[0x440968]c:\windows\explorer.exe◆
◆◆Time=[0x440968]04/01/2011 13:00:05◆
◆◆Focus=[0xB021A]Adobe Photoshop CS3 Extended◆
◆◆Executable=[0xB021A]c:\program files\adobe\adobe photoshop cs3\photoshop.exe◆
◆◆Time=[0xB021A]04/01/2011 13:00:09◆
◆◆Password◆◆◆EndPass◆◆◆Spec=Ctrl+Z◆◆◆Password◆◆◆EndPass◆◆◆Spec=Alt+Backspace◆◆◆Spec=Ctrl+D◆◆◆Spec=Ctrl
◆◆Executable=[0x8078C]c:\program files\adobe\adobe indesign cs3\indesign.exe◆
◆◆Time=[0x8078C]04/01/2011 13:03:00◆
◆◆Spec=Ctrl+Z◆◆◆Spec=Ctrl+Z◆◆◆Spec=Ctrl+Z◆◆◆Spec=Space◆◆◆Spec=Ctrl+Z◆◆◆Spec=Space◆◆◆Spec=DELETE◆◆◆Spec
```

Quality:Good Type:PINWALE/HTTP/Text Codeset:UTF-8 Attachments:0 Highlights:0 Search Hits:0

Document display complete(no highlights found)

(U) UIS



#	Folder Name
1	Shared
2	Personal
3	Print Queue

#	DBTYPE	UNIVERSA...	Rav
49	YNKE	6e3ea...	23
50	YNKE	35def...	23
51	YNKE	ee1d75...	23
52	YNKE	ee1d75...	23
53	YNKE	ee1d75...	23
54	YNKE	c713ce...	23
55	YNKE	29b7e9...	23
56	YNKE	d7e6d3...	23
57	YNKE	249fe8...	23
58	YNKE	ee1d75...	23
59	YNKE	ee1d75...	23
60	YNKE	ee1d75...	23
61	YNKE	ee1d75...	23
62	YNKE	419135...	23
63	YNKE	419135...	23
64	YNKE	419135...	23
65	YNKE	419135...	23
66	YNKE	1ad52b...	23
67	YNKE	1ad52b...	23

Item Count: 100 Selected Ite

Prioritization: None

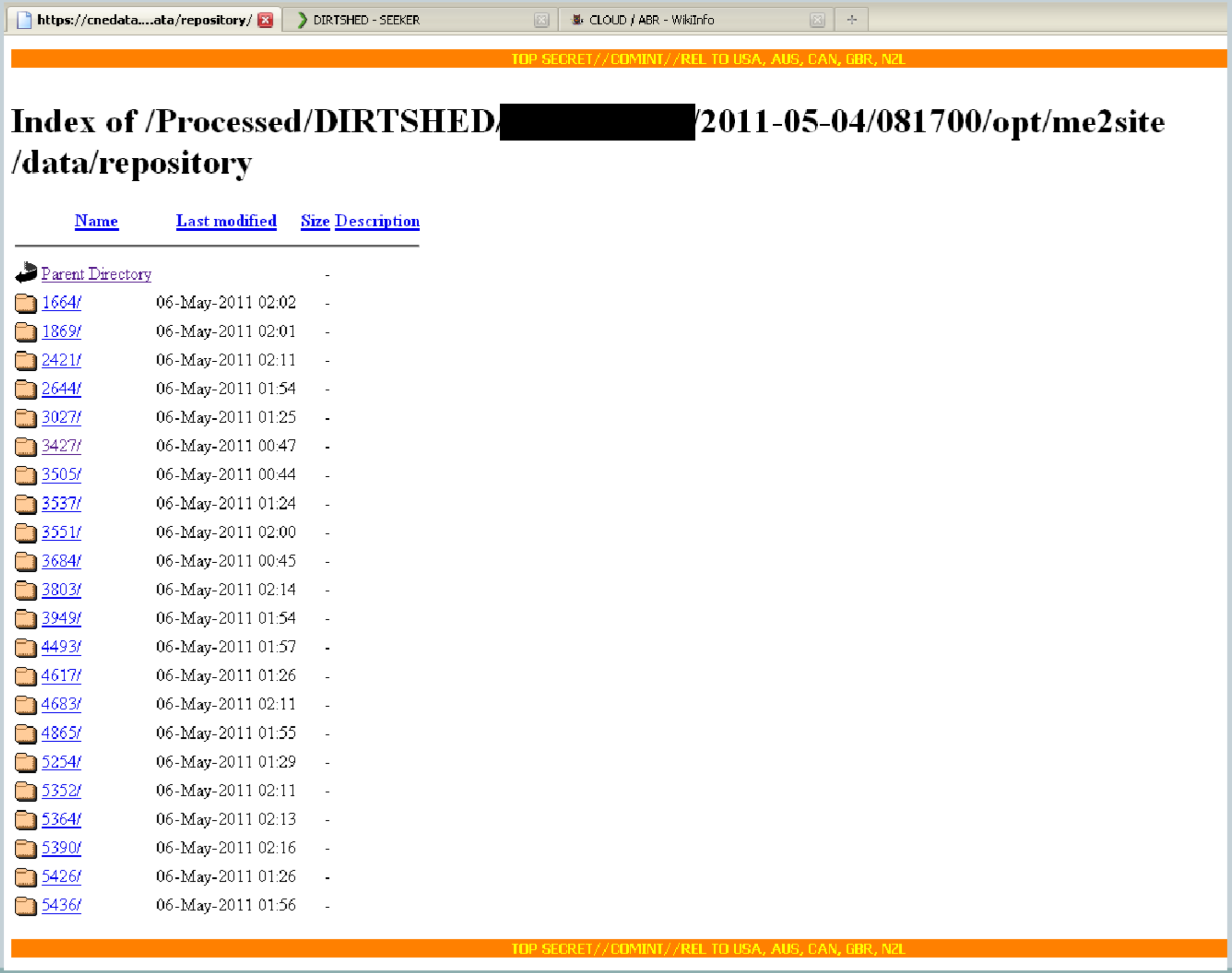
```
HTTP/1.0 200 OK
Content-Disposition:  J:\s1196594477.jpg
Content-Type:         image/jpeg
```

Displaying image 1 of 1

Quality: Good | Type: PINWALE/HTTP/Image-JPEG | Codeset: ISO8859_1 | Attachments: 0 | Highlights: 0 | Search Hits: 0

Document display complete(no highlights found)

(U) TUNINGFORK



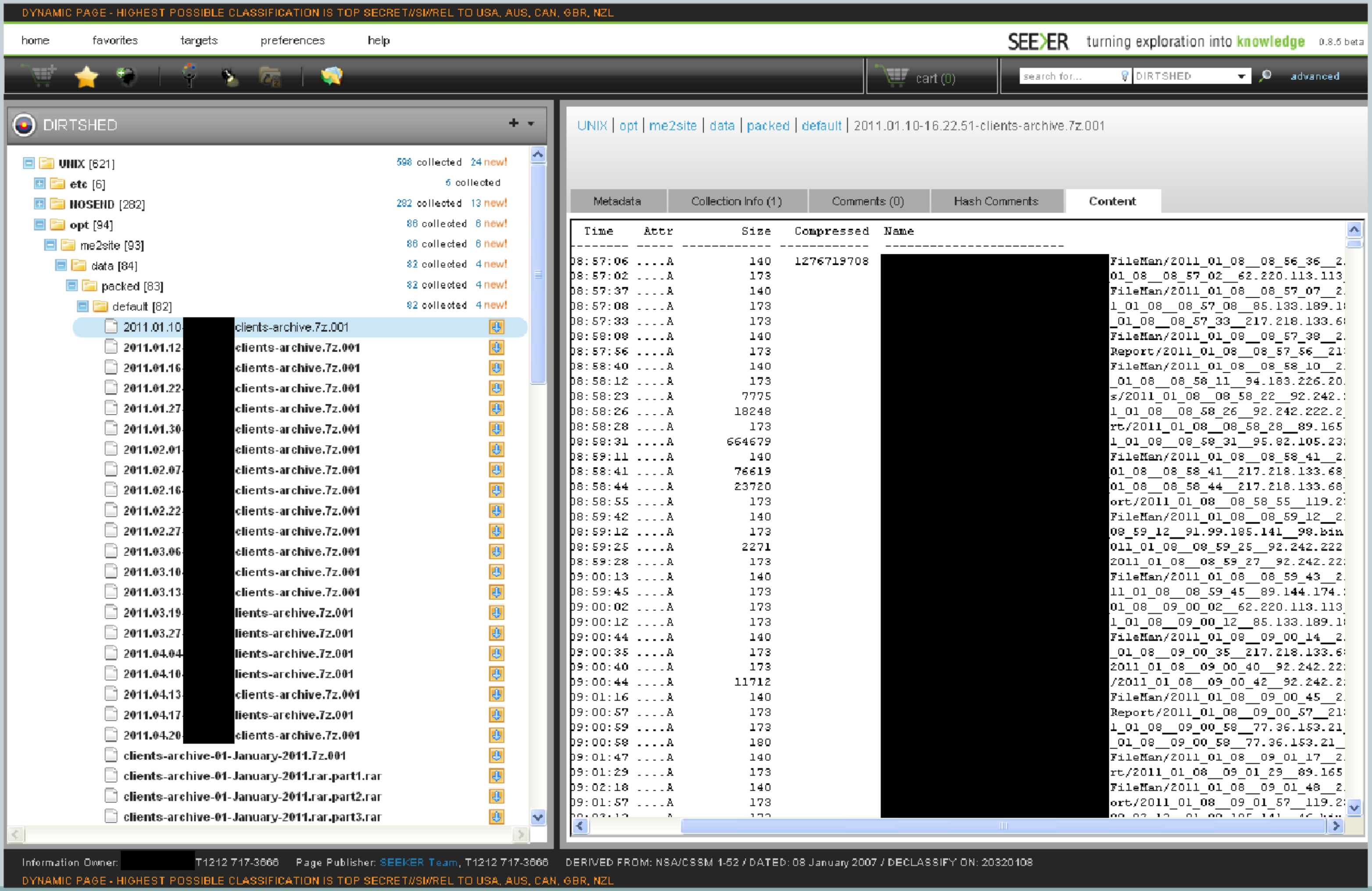
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Index of /Processed/DIRTSHED/[redacted]/2011-05-04/081700/opt/me2site/data/repository

Name	Last modified	Size	Description
Parent Directory		-	
1664/	06-May-2011 02:02	-	
1869/	06-May-2011 02:01	-	
2421/	06-May-2011 02:11	-	
2644/	06-May-2011 01:54	-	
3027/	06-May-2011 01:25	-	
3427/	06-May-2011 00:47	-	
3505/	06-May-2011 00:44	-	
3537/	06-May-2011 01:24	-	
3551/	06-May-2011 02:00	-	
3684/	06-May-2011 00:45	-	
3803/	06-May-2011 02:14	-	
3949/	06-May-2011 01:54	-	
4493/	06-May-2011 01:57	-	
4617/	06-May-2011 01:26	-	
4683/	06-May-2011 02:11	-	
4865/	06-May-2011 01:55	-	
5254/	06-May-2011 01:29	-	
5352/	06-May-2011 02:11	-	
5364/	06-May-2011 02:13	-	
5390/	06-May-2011 02:16	-	
5426/	06-May-2011 01:26	-	
5436/	06-May-2011 01:56	-	

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

(U) SEEKER



DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

DIRTSHED

```
UNIX [621]                                  598 collected  24 new!
  etc [6]                                     6 collected
  NOSEND [282]                              282 collected  13 new!
  opt [94]                                   86 collected   6 new!
    me2site [93]                             86 collected   6 new!
      data [84]                              82 collected   4 new!
        packed [83]                          82 collected   4 new!
          default [82]                       82 collected   4 new!
            2011.01.10-[redacted]clients-archive.7z.001
            2011.01.12-clients-archive.7z.001
            2011.01.16-clients-archive.7z.001
            2011.01.22-clients-archive.7z.001
            2011.01.27-clients-archive.7z.001
            2011.01.30-clients-archive.7z.001
            2011.02.01-clients-archive.7z.001
            2011.02.07-clients-archive.7z.001
            2011.02.16-clients-archive.7z.001
            2011.02.22-clients-archive.7z.001
            2011.02.27-clients-archive.7z.001
            2011.03.06-clients-archive.7z.001
            2011.03.10-clients-archive.7z.001
            2011.03.13-clients-archive.7z.001
            2011.03.19-lients-archive.7z.001
            2011.03.27-lients-archive.7z.001
            2011.04.04-lients-archive.7z.001
            2011.04.10-lients-archive.7z.001
            2011.04.13-clients-archive.7z.001
            2011.04.17-lients-archive.7z.001
            2011.04.20-clients-archive.7z.001
            clients-archive-01-January-2011.7z.001
            clients-archive-01-January-2011.rar.part1.rar
            clients-archive-01-January-2011.rar.part2.rar
            clients-archive-01-January-2011.rar.part3.rar
```

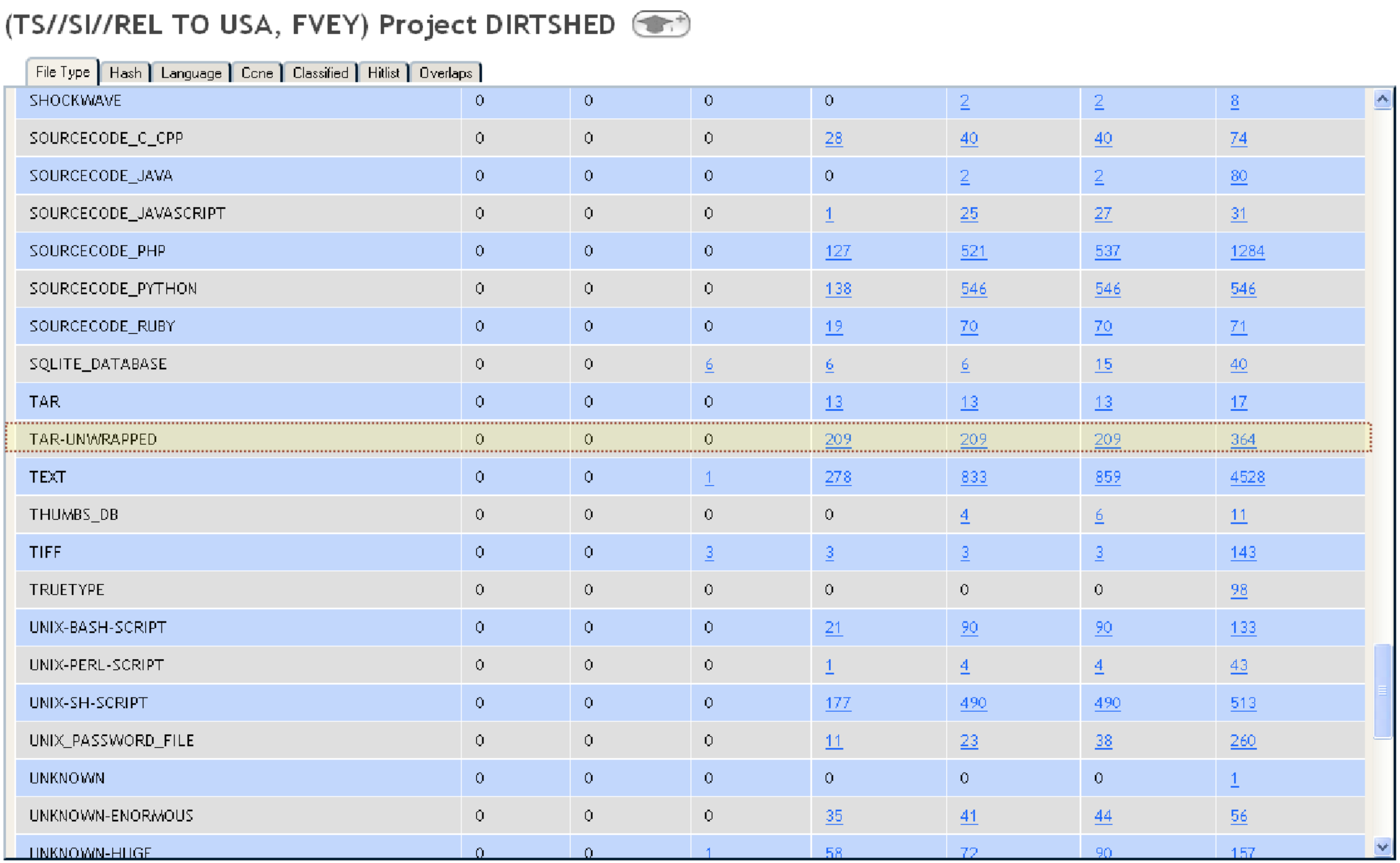
UNIX | opt | me2site | data | packed | default | 2011.01.10-16.22.51-clients-archive.7z.001

```
 Time     Attr         Size   Compressed  Name
-------- ----- ------------ ------------  ------------------------
08:57:06 ....A          140   1276719708  [redacted]FileMan/2011_01_08__08_56_36__2.
08:57:02 ....A          173               01_08__08_57_02__62.220.113.113
08:57:37 ....A          140               FileMan/2011_01_08__08_57_07__2.
08:57:08 ....A          173               1_01_08__08_57_08__85.133.189.1
08:57:33 ....A          173               _01_08__08_57_33__217.218.133.6
08:58:08 ....A          140               FileMan/2011_01_08__08_57_38__2.
08:57:56 ....A          173               Report/2011_01_08__08_57_56__21
08:58:40 ....A          140               FileMan/2011_01_08__08_58_10__2.
08:58:12 ....A          173               _01_08__08_58_11__94.183.226.20.
08:58:23 ....A         7775               s/2011_01_08__08_58_22__92.242.
08:58:26 ....A        18248               1_01_08__08_58_26__92.242.222.2
08:58:28 ....A          173               rt/2011_01_08__08_58_28__89.165
08:58:31 ....A       664679               1_01_08__08_58_31__95.82.105.23
08:59:11 ....A          140               FileMan/2011_01_08__08_58_41__2.
08:58:41 ....A        76619               01_08__08_58_41__217.218.133.68
08:58:44 ....A        23720               01_08__08_58_44__217.218.133.68
08:58:55 ....A          173               ort/2011_01_08__08_58_55__119.2
08:59:42 ....A          140               FileMan/2011_01_08__08_59_12__2.
08:59:12 ....A          173               08_59_12__91.99.185.141__98.bin
08:59:25 ....A         2271               011_01_08__08_59_25__92.242.222
08:59:28 ....A          173               2011_01_08__08_59_27__92.242.22
09:00:13 ....A          140               FileMan/2011_01_08__08_59_43__2.
08:59:45 ....A          173               11_01_08__08_59_45__89.144.174.
09:00:02 ....A          173               01_08__09_00_02__62.220.113.113
09:00:12 ....A          173               1_01_08__09_00_12__85.133.189.1
09:00:44 ....A          140               FileMan/2011_01_08__09_00_14__2.
09:00:35 ....A          173               _01_08__09_00_35__217.218.133.6
09:00:40 ....A          173               2011_01_08__09_00_40__92.242.22
09:00:44 ....A        11712               /2011_01_08__09_00_42__92.242.2
09:01:16 ....A          140               FileMan/2011_01_08__09_00_45__2.
09:00:57 ....A          173               Report/2011_01_08__09_00_57__21
09:00:59 ....A          173               1_01_08__09_00_58__77.36.153.21_
09:00:58 ....A          180               _01_08__09_00_58__77.36.153.21_
09:01:47 ....A          140               FileMan/2011_01_08__09_01_17__2.
09:01:29 ....A          173               rt/2011_01_08__09_01_29__89.165
09:02:18 ....A          140               FileMan/2011_01_08__09_01_48__2.
09:01:57 ....A          173               ort/2011_01_08__09_01_57__119.2
```

Information Owner: [redacted] T1212 717-3666   Page Publisher: SEEKER Team, T1212 717-3666   DERIVED FROM: NSA/CSSM 1-52 / DATED: 08 January 2007 / DECLASSIFY ON: 20320108

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

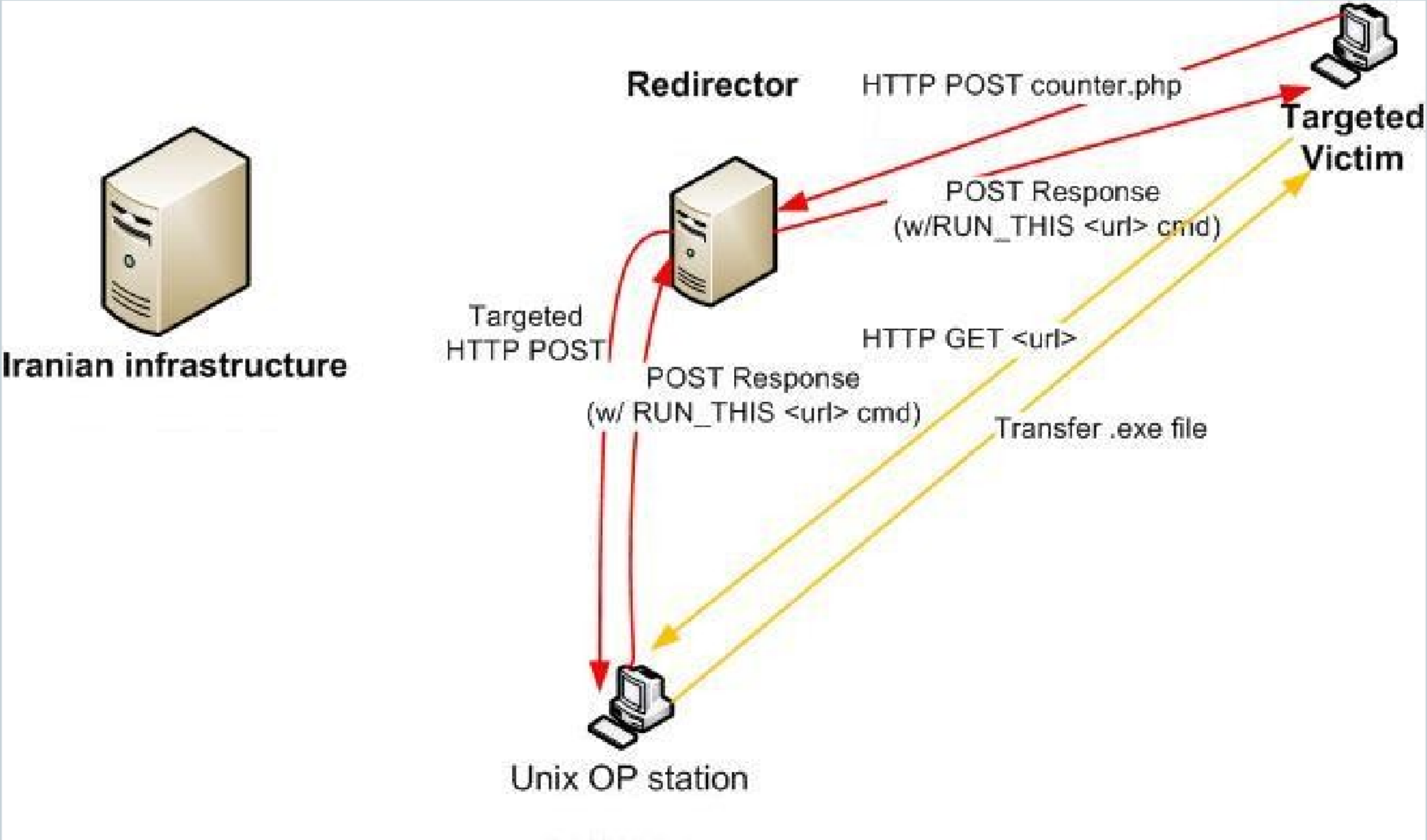
(U) Cloud/ABR



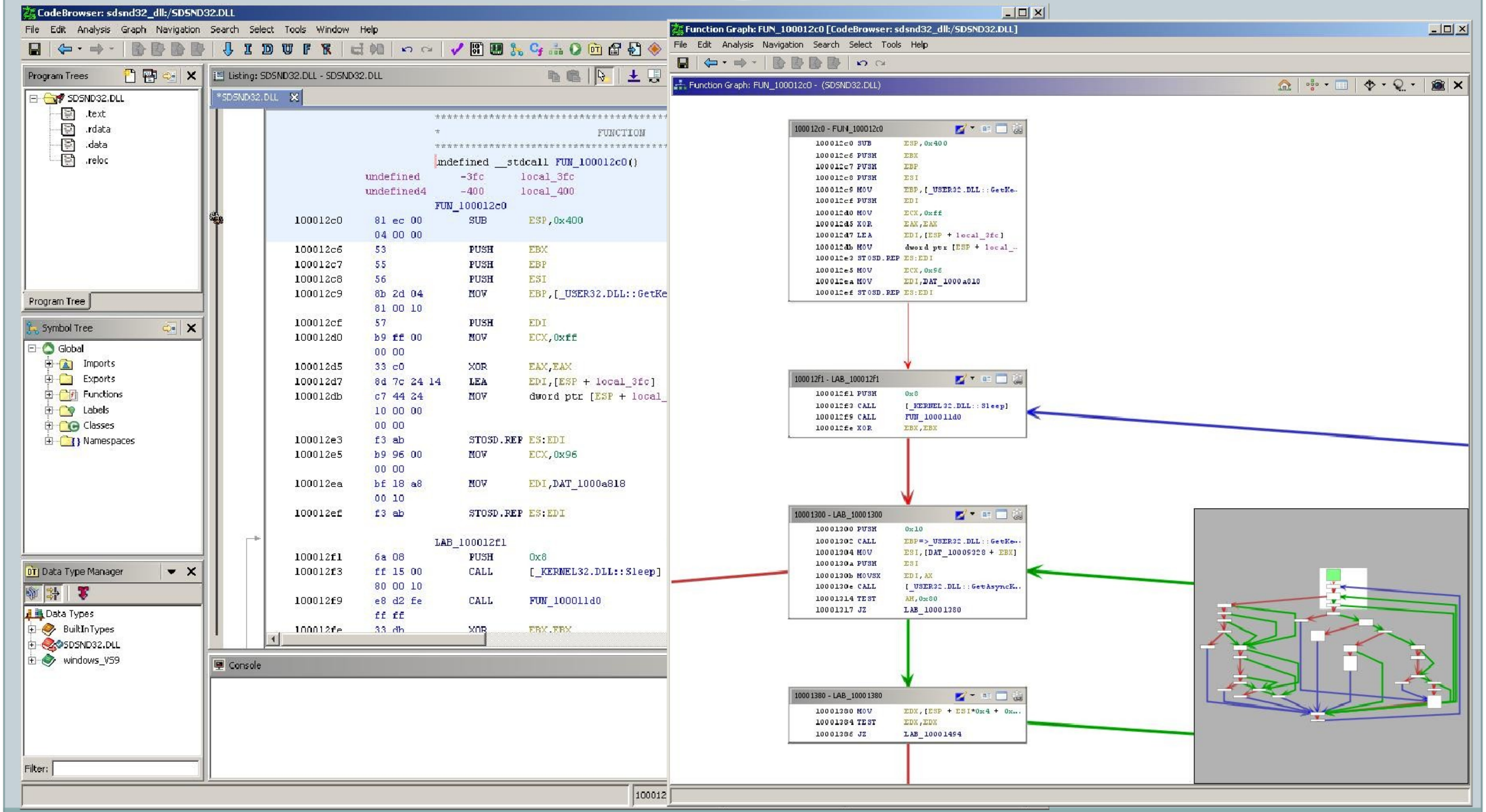
(TS//SI//REL TO USA, FVEY) Project DIRTSHED

SHOCKWAVE	0	0	0	0	2	2	8
SOURCECODE_C_CPP	0	0	0	28	40	40	74
SOURCECODE_JAVA	0	0	0	0	2	2	80
SOURCECODE_JAVASCRIPT	0	0	0	1	25	27	31
SOURCECODE_PHP	0	0	0	127	521	537	1284
SOURCECODE_PYTHON	0	0	0	138	546	546	546
SOURCECODE_RUBY	0	0	0	19	70	70	71
SQLITE_DATABASE	0	0	6	6	6	15	40
TAR	0	0	0	13	13	13	17
TAR-UNWRAPPED	0	0	0	209	209	209	364
TEXT	0	0	1	278	833	859	4528
THUMBS_DB	0	0	0	0	4	6	11
TIFF	0	0	3	3	3	3	143
TRUETYPE	0	0	0	0	0	0	98
UNIX-BASH-SCRIPT	0	0	0	21	90	90	133
UNIX-PERL-SCRIPT	0	0	0	1	4	4	43
UNIX-SH-SCRIPT	0	0	0	177	490	490	513
UNIX_PASSWORD_FILE	0	0	0	11	23	38	260
UNKNOWN	0	0	0	0	0	0	1
UNKNOWN-ENORMOUS	0	0	0	35	41	44	56
UNKNOWN-HUGE	0	0	1	58	72	90	157

(TS//SI//REL) Example: Victim Stealing



(U//FOUO) Repurposing


CodeBrowser: sdsnd32_dll:/SDSND32.DLL
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
SDSND32.DLL
.text
.rdata
.data
.reloc
Program Tree
Symbol Tree
Global
Imports
Exports
Functions
Labels
Classes
Namespaces
Data Type Manager
Data Types
BuiltInTypes
SDSND32.DLL
windows_VS9
Filter:
Listing: SDSND32.DLL - SDSND32.DLL
*SDSND32.DLL
Console
100012
Function Graph: FUN_100012c0 [CodeBrowser: sdsnd32_dll:/SDSND32.DLL]
File Edit Analysis Navigation Search Select Tools Help
Function Graph: FUN_100012c0 - (SDSND32.DLL)

```
                              ****************************************
                              *                   FUNCTION
                              ****************************************
                              undefined __stdcall FUN_100012c0()
              undefined         -3fc        local_3fc
              undefined4        -400        local_400
                              FUN_100012c0
    100012c0      81 ec 00        SUB       ESP,0x400
                  04 00 00
    100012c6      53              PUSH      EBX
    100012c7      55              PUSH      EBP
    100012c8      56              PUSH      ESI
    100012c9      8b 2d 04        MOV       EBP,[_USER32.DLL::GetKe
                  81 00 10
    100012cf      57              PUSH      EDI
    100012d0      b9 ff 00        MOV       ECX,0xff
                  00 00
    100012d5      33 c0           XOR       EAX,EAX
    100012d7      8d 7c 24 14     LEA       EDI,[ESP + local_3fc]
    100012db      c7 44 24        MOV       dword ptr [ESP + local_
                  10 00 00
                  00 00
    100012e3      f3 ab           STOSD.REP ES:EDI
    100012e5      b9 96 00        MOV       ECX,0x96
                  00 00
    100012ea      bf 18 a8        MOV       EDI,DAT_1000a818
                  00 10
    100012ef      f3 ab           STOSD.REP ES:EDI

                              LAB_100012f1
    100012f1      6a 08           PUSH      0x8
    100012f3      ff 15 00        CALL      [_KERNEL32.DLL::Sleep]
                  80 00 10
    100012f9      e8 d2 fe        CALL      FUN_100011d0
                  ff ff
    100012fe      33 db           XOR       EBX,EBX
```

```
100012c0 - FUN_100012c0
    100012c0 SUB        ESP,0x400
    100012c6 PUSH       EBX
    100012c7 PUSH       EBP
    100012c8 PUSH       ESI
    100012c9 MOV        EBP,[_USER32.DLL::GetKe…
    100012cf PUSH       EDI
    100012d0 MOV        ECX,0xff
    100012d5 XOR        EAX,EAX
    100012d7 LEA        EDI,[ESP + local_3fc]
    100012db MOV        dword ptr [ESP + local_…
    100012e3 STOSD.REP  ES:EDI
    100012e5 MOV        ECX,0x96
    100012ea MOV        EDI,DAT_1000a818
    100012ef STOSD.REP  ES:EDI
```

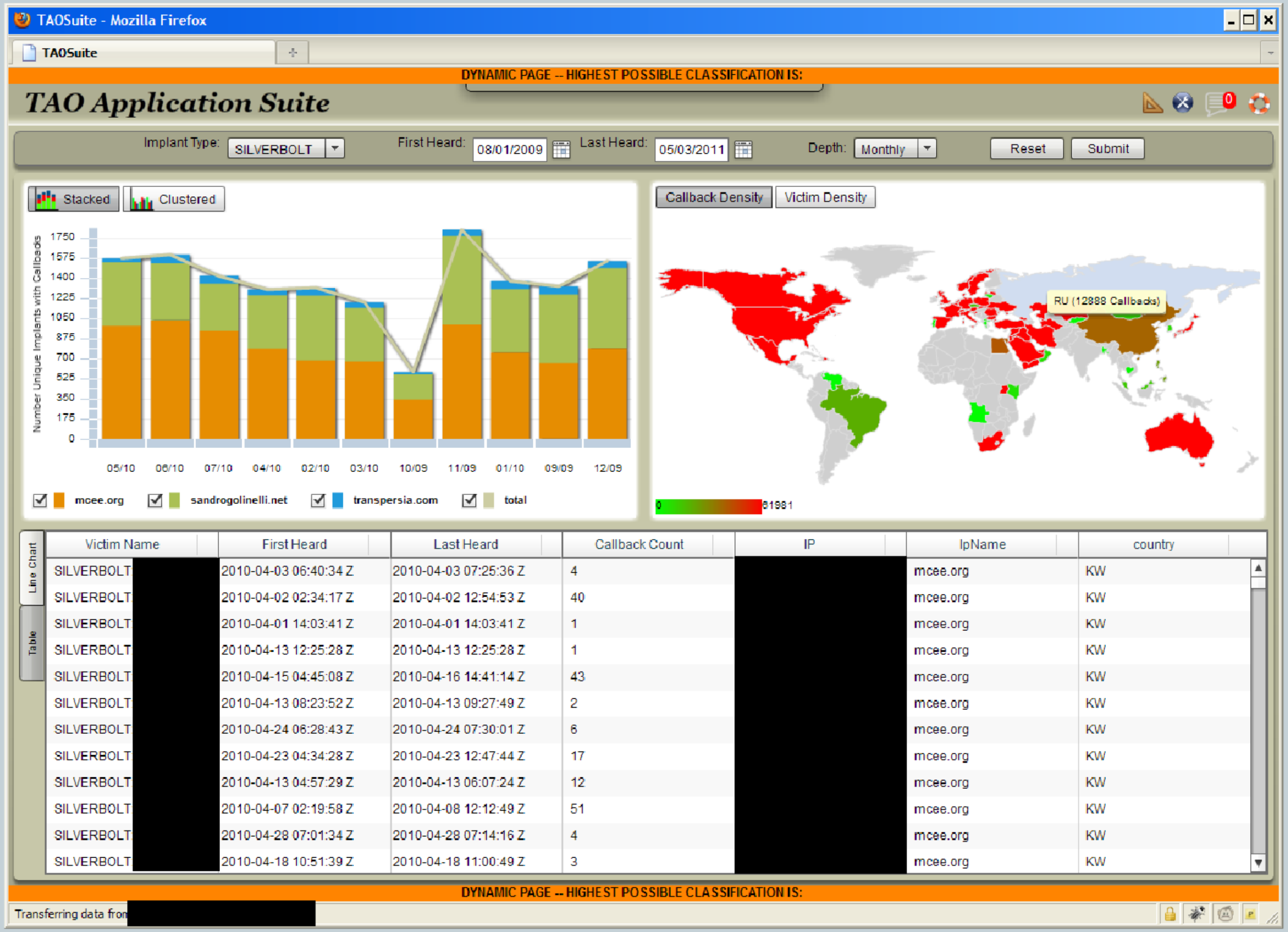
```
100012f1 - LAB_100012f1
    100012f1 PUSH       0x8
    100012f3 CALL       [_KERNEL32.DLL::Sleep]
    100012f9 CALL       FUN_100011d0
    100012fe XOR        EBX,EBX
```

```
10001300 - LAB_10001300
    10001300 PUSH       0x10
    10001302 CALL       EBP=>_USER32.DLL::GetKe…
    10001304 MOV        ESI,[DAT_10009328 + EBX]
    1000130a PUSH       ESI
    1000130b MOVSX      EDI,AX
    1000130e CALL       [_USER32.DLL::GetAsyncK…
    10001314 TEST       AH,0x80
    10001317 JZ         LAB_10001380
```

```
10001380 - LAB_10001380
    10001380 MOV        EDX,[ESP + ESI*0x4 + 0x…
    10001384 TEST       EDX,EDX
    10001386 JZ         LAB_10001494
```

(U) Current Efforts

(U) VicDB



DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS:

Implant Type: SILVERBOLT First Heard: 08/01/2009 Last Heard: 05/03/2011 Depth: Monthly Reset Submit

☑ 🟧 mcee.org ☑ 🟩 sandrogolinelli.net ☑ 🟦 transpersia.com ☑ ▨ total

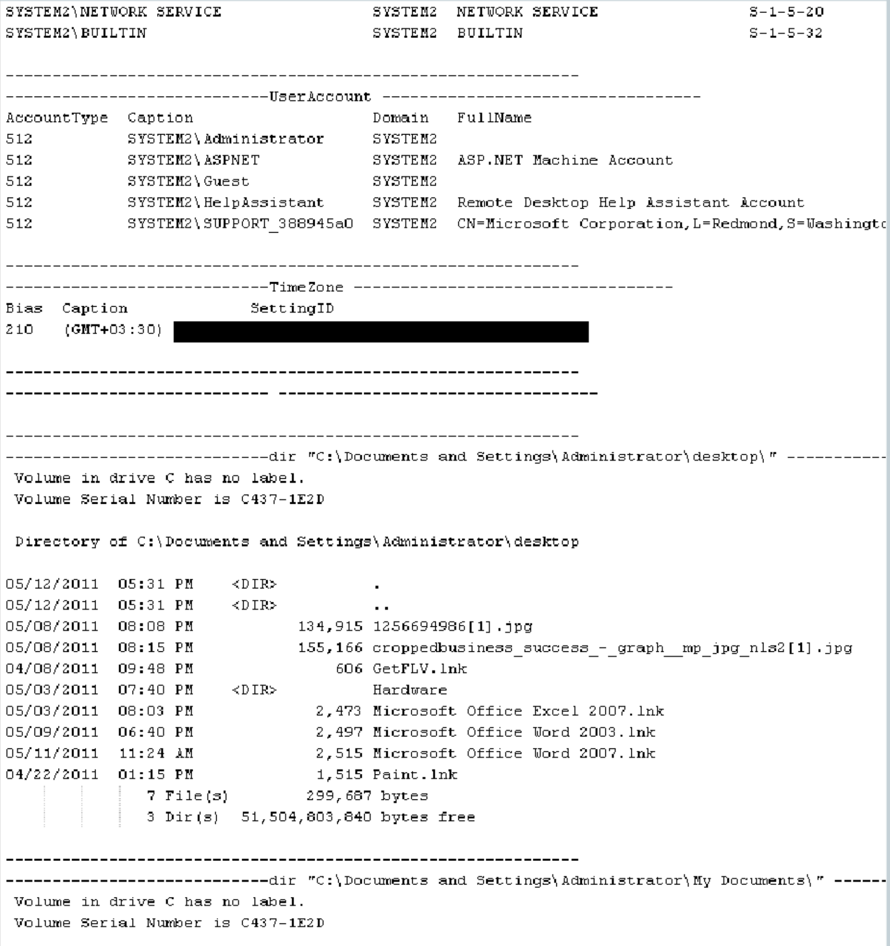
Line Chart | Table

Victim Name	First Heard	Last Heard	Callback Count	IP	IpName	country
SILVERBOLT [redacted]	2010-04-03 06:40:34 Z	2010-04-03 07:25:36 Z	4	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-02 02:34:17 Z	2010-04-02 12:54:53 Z	40	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-01 14:03:41 Z	2010-04-01 14:03:41 Z	1	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-13 12:25:28 Z	2010-04-13 12:25:28 Z	1	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-15 04:45:08 Z	2010-04-16 14:41:14 Z	43	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-13 08:23:52 Z	2010-04-13 09:27:49 Z	2	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-24 06:28:43 Z	2010-04-24 07:30:01 Z	6	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-23 04:34:28 Z	2010-04-23 12:47:44 Z	17	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-13 04:57:29 Z	2010-04-13 06:07:24 Z	12	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-07 02:19:58 Z	2010-04-08 12:12:49 Z	51	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-28 07:01:34 Z	2010-04-28 07:14:16 Z	4	[redacted]	mcee.org	KW
SILVERBOLT [redacted]	2010-04-18 10:51:39 Z	2010-04-18 11:00:49 Z	3	[redacted]	mcee.org	KW

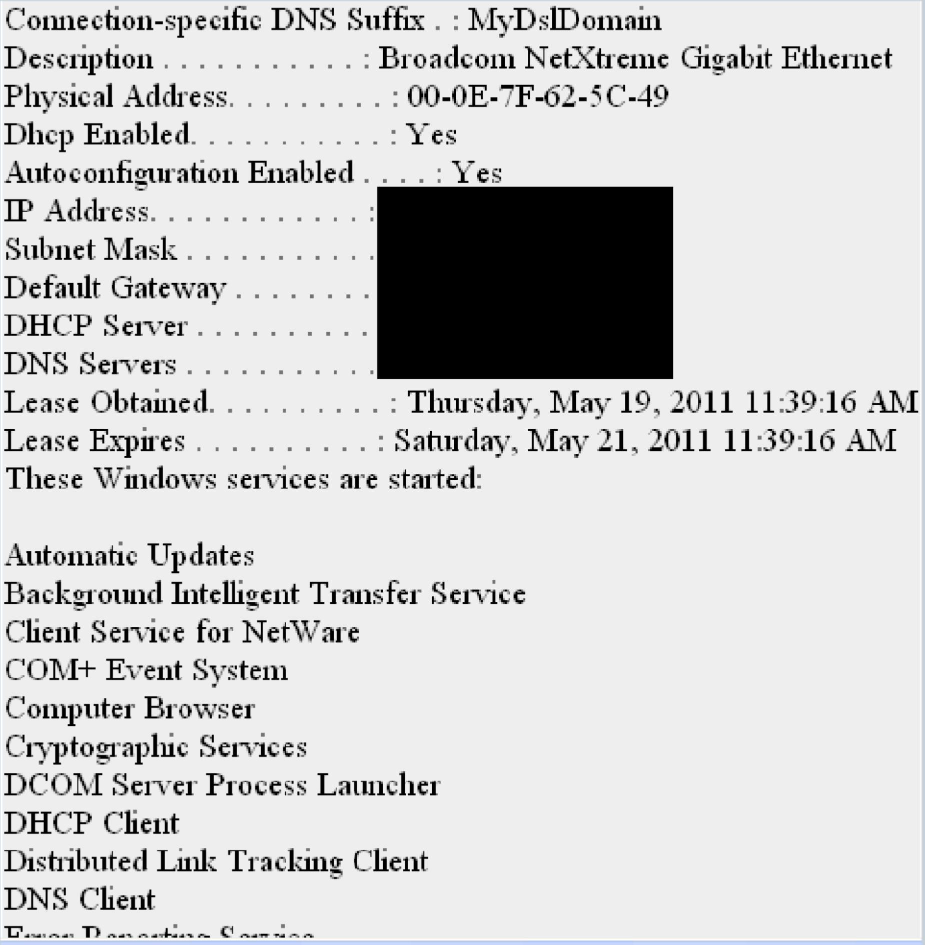
DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS:

Transferring data fro [redacted]

(S//SI) Survey Data

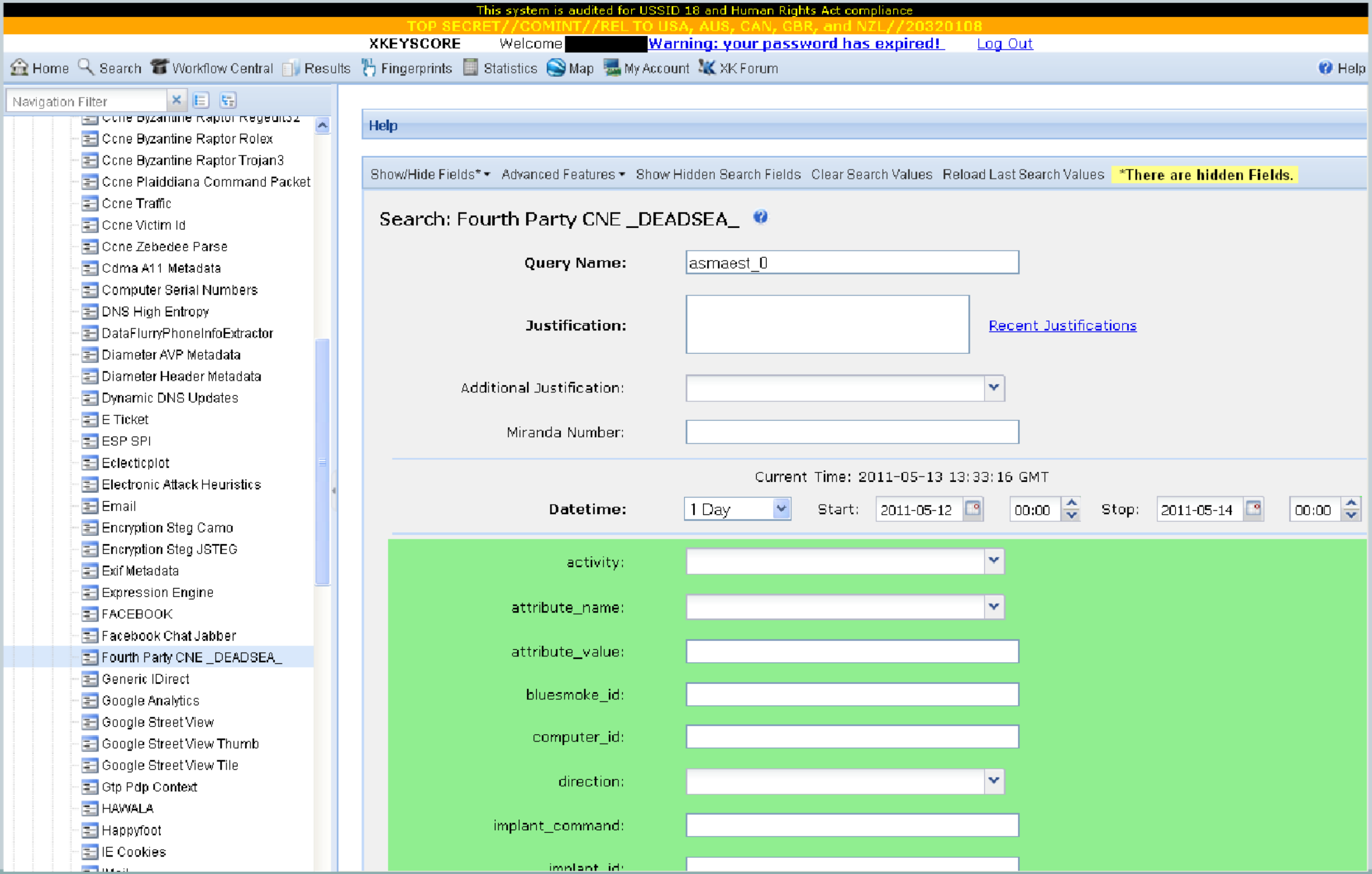


```
SYSTEM2\NETWORK SERVICE                          SYSTEM2  NETWORK SERVICE                        S-1-5-20
SYSTEM2\BUILTIN                                  SYSTEM2  BUILTIN                                S-1-5-32

------------------------------------------------------------
----------------------------UserAccount ----------------------------------
AccountType  Caption                   Domain   FullName
512          SYSTEM2\Administrator     SYSTEM2
512          SYSTEM2\ASPNET            SYSTEM2  ASP.NET Machine Account
512          SYSTEM2\Guest             SYSTEM2
512          SYSTEM2\HelpAssistant     SYSTEM2  Remote Desktop Help Assistant Account
512          SYSTEM2\SUPPORT_388945a0  SYSTEM2  CN=Microsoft Corporation,L=Redmond,S=Washingto

------------------------------------------------------------
----------------------------TimeZone ----------------------------------
Bias  Caption               SettingID
210   (GMT+03:30) [redacted]

------------------------------------------------------------
---------------------------- ------------------------------------

------------------------------------------------------------
----------------------------dir "C:\Documents and Settings\Administrator\desktop\" -----------
 Volume in drive C has no label.
 Volume Serial Number is C437-1E2D

 Directory of C:\Documents and Settings\Administrator\desktop

05/12/2011  05:31 PM    <DIR>          .
05/12/2011  05:31 PM    <DIR>          ..
05/08/2011  08:08 PM           134,915 1256694986[1].jpg
05/08/2011  08:15 PM           155,166 croppedbusiness_success_-_graph__mp_jpg_nls2[1].jpg
04/08/2011  09:48 PM               606 GetFLV.lnk
05/03/2011  07:40 PM    <DIR>          Hardware
05/03/2011  08:03 PM             2,473 Microsoft Office Excel 2007.lnk
05/09/2011  06:40 PM             2,497 Microsoft Office Word 2003.lnk
05/11/2011  11:24 AM             2,515 Microsoft Office Word 2007.lnk
04/22/2011  01:15 PM             1,515 Paint.lnk
               7 File(s)        299,687 bytes
               3 Dir(s)  51,504,803,840 bytes free

------------------------------------------------------------
----------------------------dir "C:\Documents and Settings\Administrator\My Documents\" ------
 Volume in drive C has no label.
 Volume Serial Number is C437-1E2D
```



```
Connection-specific DNS Suffix  . : MyDslDomain
Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
Physical Address. . . . . . . . . : 00-0E-7F-62-5C-49
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : [redacted]
Subnet Mask . . . . . . . . . . .
Default Gateway . . . . . . . . .
DHCP Server . . . . . . . . . . .
DNS Servers . . . . . . . . . . .
Lease Obtained. . . . . . . . . . : Thursday, May 19, 2011 11:39:16 AM
Lease Expires . . . . . . . . . . : Saturday, May 21, 2011 11:39:16 AM
These Windows services are started:

Automatic Updates
Background Intelligent Transfer Service
Client Service for NetWare
COM+ Event System
Computer Browser
Cryptographic Services
DCOM Server Process Launcher
DHCP Client
Distributed Link Tracking Client
DNS Client
Error Reporting Service
```

(U) DEADSEA



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] Warning: your password has expired! Log Out

- Ccne Byzantine Raptor Regeuits2
- Ccne Byzantine Raptor Rolex
- Ccne Byzantine Raptor Trojan3
- Ccne Plaiddiana Command Packet
- Ccne Traffic
- Ccne Victim Id
- Ccne Zebedee Parse
- Cdma A11 Metadata
- Computer Serial Numbers
- DNS High Entropy
- DataFlurryPhoneInfoExtractor
- Diameter AVP Metadata
- Diameter Header Metadata
- Dynamic DNS Updates
- E Ticket
- ESP SPI
- Eclecticplot
- Electronic Attack Heuristics
- Email
- Encryption Steg Camo
- Encryption Steg JSTEG
- Exif Metadata
- Expression Engine
- FACEBOOK
- Facebook Chat Jabber
- Fourth Party CNE _DEADSEA_
- Generic IDirect
- Google Analytics
- Google Street View
- Google Street View Thumb
- Google Street View Tile
- Gtp Pdp Context
- HAWALA
- Happyfoot
- IE Cookies
- IMail

*There are hidden Fields.

Search: Fourth Party CNE _DEADSEA_

Query Name: asmaest_0

Justification:

Additional Justification:

Miranda Number:

Current Time: 2011-05-13 13:33:16 GMT

Datetime: 1 Day Start: 2011-05-12 00:00 Stop: 2011-05-14 00:00

activity:

attribute_name:

attribute_value:

bluesmoke_id:

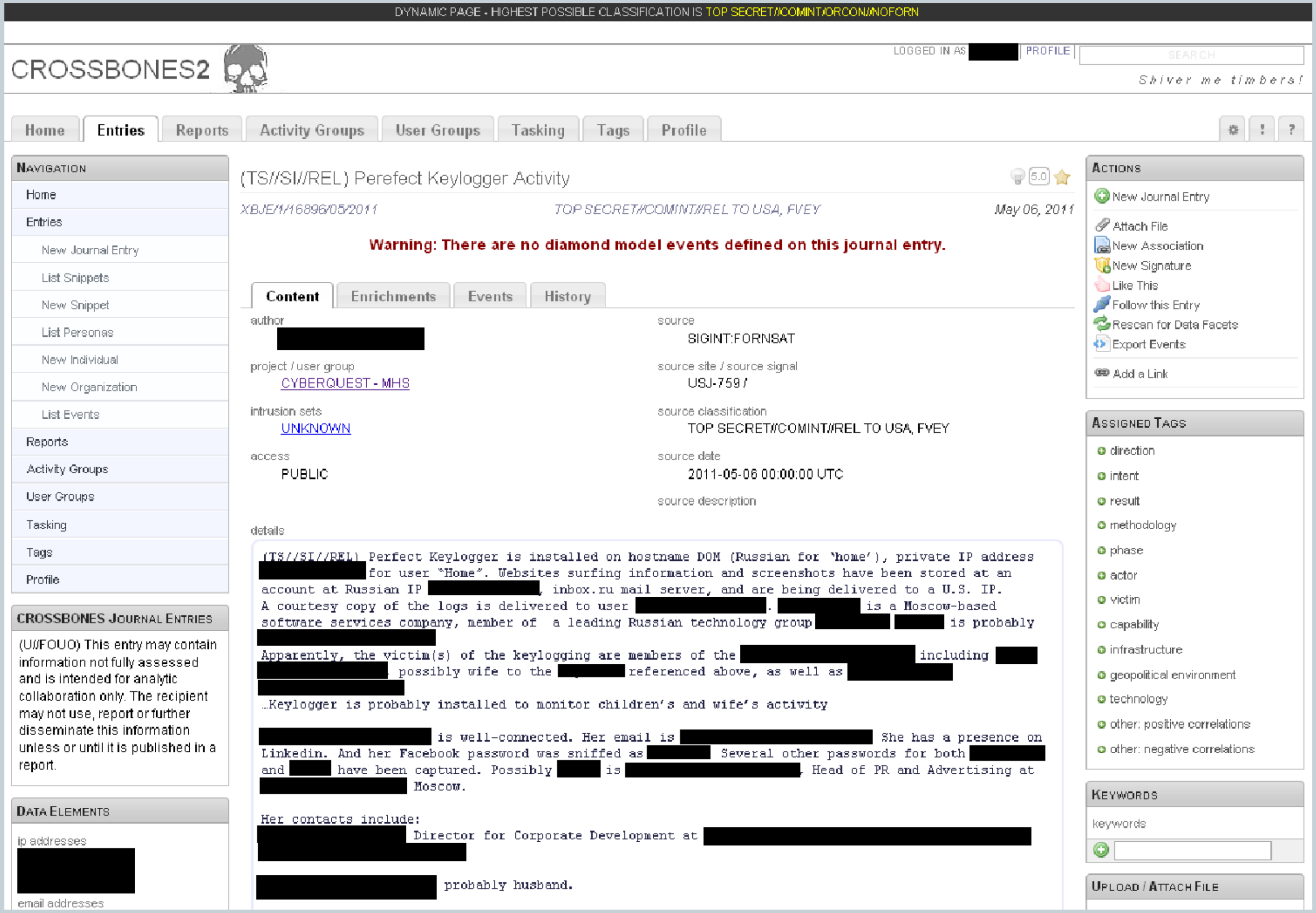
computer_id:

direction:

implant_command:

implant_id:

(S//SI) Discovery for 4th Party



DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//COMINT/ORCON/NOFORN

CROSSBONES2

LOGGED IN AS [redacted] | PROFILE | SEARCH

Shiver me timbers!

NAVIGATION

CROSSBONES JOURNAL ENTRIES

(U//FOUO) This entry may contain information not fully assessed and is intended for analytic collaboration only. The recipient may not use, report or further disseminate this information unless or until it is published in a report.

DATA ELEMENTS

ip addresses
[redacted]

email addresses

(TS//SI//REL) Perefect Keylogger Activity

5.0

XBJE/1/16896/05/2011 TOP SECRET//COMINT//REL TO USA, FVEY May 06, 2011

Warning: There are no diamond model events defined on this journal entry.

author
[redacted]

project / user group
CYBERQUEST - MHS

intrusion sets
UNKNOWN

access
PUBLIC

source
SIGINT:FORNSAT

source site / source signal
USJ-759 /

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

source date
2011-05-06 00:00:00 UTC

source description

details

```
(TS//SI//REL) Perfect Keylogger is installed on hostname DOM (Russian for 'home'), private IP address
[redacted] for user "Home". Websites surfing information and screenshots have been stored at an
account at Russian IP [redacted], inbox.ru mail server, and are being delivered to a U.S. IP.
A courtesy copy of the logs is delivered to user [redacted]. [redacted] is a Moscow-based
software services company, member of  a leading Russian technology group [redacted] [redacted] is probably
[redacted]
Apparently, the victim(s) of the keylogging are members of the [redacted] including [redacted]
[redacted] possibly wife to the [redacted] referenced above, as well as [redacted]
[redacted]
…Keylogger is probably installed to monitor children's and wife's activity

[redacted] is well-connected. Her email is [redacted] She has a presence on
Linkedin. And her Facebook password was sniffed as [redacted] Several other passwords for both [redacted]
and [redacted] have been captured. Possibly [redacted] is [redacted], Head of PR and Advertising at
[redacted] Moscow.

Her contacts include:
[redacted] Director for Corporate Development at [redacted]
[redacted]

[redacted] probably husband.
```

ACTIONS

ASSIGNED TAGS

- direction
- intent
- result
- methodology
- phase
- actor
- victim
- capability
- infrastructure
- geopolitical environment
- technology
- other: positive correlations
- other: negative correlations

KEYWORDS

keywords

UPLOAD / ATTACH FILE

Contact us

EMAIL: DL 4THPARTY

NSANET: GO 4THPARTY

JABBER: S2 CYBER ANALYSIS