

Computer Forensic Analysis

***A look at some of the general steps used
in conducting a computer forensic examination:***

Communication!!!



A Friendly Reminder...

"If computer evidence in a criminal case is received without a valid copy of the original chain of custody/evidence receipt it will immediately be sent back to the submitting party or agency. This requirement applies to any agency or person (including members of the USDA-OIG) submitting evidence to the NCFU in regard to a criminal case. In addition to a valid copy of the original chain of custody/evidence receipt, a completed copy of the NCFU Request for Service form (see attached exhibit 1) must be submitted. The completed NCFU Request for Service form contains information about the case as well as information about what the submitting party (also known as the case agent) is requesting the examination be conducted in order to locate. If a case or computer evidence is submitted to the NCFU without a completed NCFU Request for Service, a member of the NCFU staff will contact the submitting party and request that the submitting party complete and submit a copy of the NCFU Request for Service form. If a completed copy of the Request for Service form is not submitted to the NCFU within a reasonable amount of time (as determined by the NCFU Supervisor), then the computer evidence will be returned to the submitting party without a computer forensic examination having been conducted."

a non criminal case

Revised: 03/27/2006

Page 2

Full Screen
Close Full Screen

The Request...

CASE INFORMATION (Please print legibly. If Not Applicable, enter "NA")		NCFU Case #
Is this the first request in this case? <input checked="" type="checkbox"/> First Request <input type="checkbox"/> Follow-up Request	Date: 05/09/2006	Agency Case # KC-0204-0099
Submitting Person: Craig Goscha	Submitting Person Phone: 816-926-7644	Suspect Name Or Case Title: Shawn Healy
Case Agent Name: Craig Goscha	Squad/Unit: NCFU	Submitting Agency: USDA-OIG
Case Agent Phone: 816-926-7644	Case Agent Email: cmgoscha@oig.usda.gov	
Service or Seizure Location (Address): 8930 Ward Parkway, Suite 3016, Kansas City, Mo 64114	Date of Seizure: 05/09/2006	Type of Seizure (Please provide a copy of Search Warrant/Affidavit) <input type="checkbox"/> Search Warrant <input type="checkbox"/> Consent <input type="checkbox"/> OIG <input checked="" type="checkbox"/> Internal <input type="checkbox"/> Grand Jury <input type="checkbox"/> Admin <input type="checkbox"/> Other
Privileged Information? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes <small>This includes any material specified under the Privacy Protection Act. For example any material intended for publication such as books, articles or computer programs</small>	Special Handling? <input type="checkbox"/> No <input type="checkbox"/> Yes <small>If any additional "Special Handling" procedures are required please describe below or attach additional pages</small>	
Were any NCFU personnel consulted <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Was Title Name(s):	Date:

Service Requested

Describe in detail what examinations are needed and what type of data you expect to be present. If there are special handling requirements, please describe. Attach additional pages as needed. If you have any reports, statements or other documentation which may assist in the examination, please attach to this request.

On 05/09/2006 OCIO contacted us in regard to firewall logs which indicated that a computer with an IP address, that resolved to a USDA computer assigned to a USDA employee, was used to access internet web pages and files that are potentially illegal or inappropriate in nature. The computer in question was located and appeared to be "powered off". The hard drive was removed and is provided for a forensic examination. Please examine the hard drive for any evidence of the receipt, manufacture or distribution of illegal or inappropriate images or videos. Additionally, please examine the hard drive for any non-government email accounts and provide the email messages for review by the case agent.

The Forensic Image: Cornerstone of Computer Forensics

The screenshot displays the EnCase Forensic application window. At the top, a menu bar includes File, Edit, View, Tools, and Help. Below it is a toolbar with icons for New, Open, Save, Print, Add Device, Search, and Refresh. A table lists acquisition items, with one entry selected:

Name	Filter	In Report	Actual Date	Target Date	File Path	Case Number	Evidence Number	Examiner Name
S1_R1_Q1_1			05/09/06 02:26:50PM	05/09/06 02:26:50PM	C:\Documents and Set PDC Presentation	S1_R1_Q1_1	S1_R1_Q1_1	Shawn Healy, FE

Below the table, the 'Device' details are shown:

Device
 Name: S1_R1_Q1_1
 Actual Date: 05/09/06 02:26:50PM
 Target Date: 05/09/06 02:26:50PM
 File Path: C:\Documents and Settings\SMHEALY\My Documents\Admin Docs\IPDC Presentation\S1_R1_Q1_1.E01
 Case Number: PDC Presentation
 Evidence Number: S1_R1_Q1_1
 Examiner Name: Shawn Healy, FE, EnCE, SCERS
 Notes: Fujitsu MHV2040AH 40GB HDD S/N: NT26T5B2W483
 Drive Type: Fixed
 File Integrity: Completely Verified 0 Errors

Two large hash values are displayed:

Acquisition Hash: fb21a750dd17a9c47f6061894b486056
 Verify Hash: fb21a750dd17a9c47f6061894b486056

Additional device statistics:

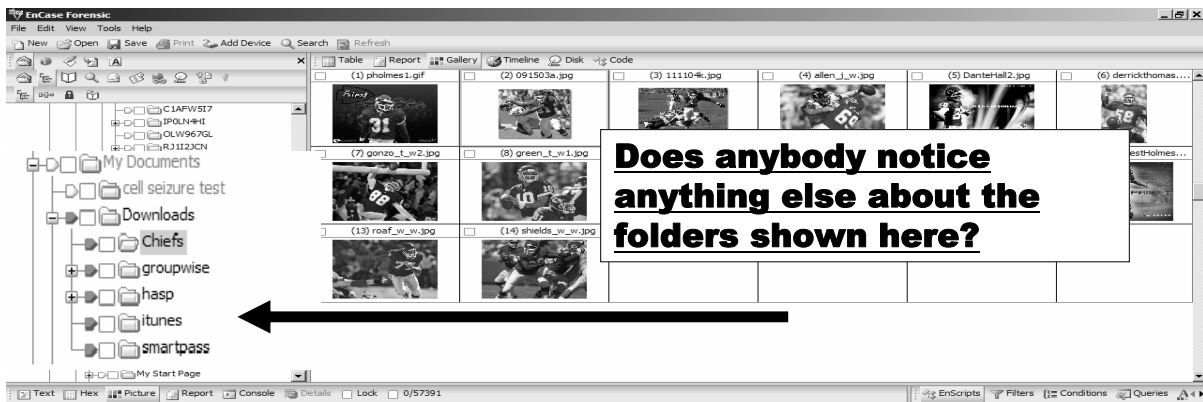
Raid Stripe Size: 0
 Error Granularity: 1
 Read Errors: 0
 CRC Errors: 0
 Compression: Best
 Total Size: 40,007,761,920 bytes (37.3GB)
 Total Sectors: 78,140,160

Partitions

Code	Type	Start Sector	Total Sectors	Size
07	NTFS	0	78,140,160	37.3GB

At the bottom, the file path is shown: PDC Presentation\S1_R1_Q1_1 (PS 0 SO 000 FO 0 LE 1)

Forensic Analysis: A Case Regarding Internet Abuse/Inappropriate or Illegal Content



All of the pictures of interest appear to be in a “user created” folder. This indicates they were intentionally saved, but where did they come from?

Next Step:

Obtain Information About the Pictures or Items of Interest

The screenshot displays the EnCase Forensic software interface. The main window shows a file list with columns for Name, Logical Size, File Created, and Hash Value. The file '091503a.jpg' is selected, and its details are shown in the preview pane below. The preview pane displays a black and white photograph of a football game, showing a player in a dark jersey (number 15) running with the ball while being tackled by a player in a light jersey (number 14). The status bar at the bottom indicates the file path: 'PDC Presentation\51_R1_Q1_1C\Documents and Settings\Shawn\My Documents\Downloads\Chiefs\091503a.jpg (PS 18384575 LS 18384512 CL 2298064 SO 000 FO 0 LE 0)'.

Name	Logical Size	File Created	Hash Value
091503a.jpg	117,792	05/09/06 01:42:09PM	f74acc650f713e2528c4d415079d90cb
alien_w.jpg	174,090	05/09/06 01:41:43PM	73c149a9a0000700204c0000000000000000
6 DanteHall2.jpg	107,332	05/09/06 01:48:10PM	cb9f1a705155a2c8bd204d3089bb944d
7 derrickthomas.jpg	9,551	05/09/06 10:17:10AM	3b97bc5146caf5cc3fcc31977770b451
8 gonzo_t_w2.jpg	165,212	05/09/06 01:40:28PM	1af9feda46d3e7e7541e54f831cdd3fb
9 green_t_w1.jpg	169,871	05/09/06 01:40:38PM	56d93c92a47f0ea2fea66fe5a04eeedf0
10 hall_def_w.jpg	172,255	05/09/06 01:40:48PM	c2b300c8e6d49750bb4d31f510f6d4e
11 holmes_w2.jpg	139,653	05/09/06 01:40:58PM	dcb8e9e1a2b46d84067a6a3a946516bc
12 priest_holmes.jpg	274,947	05/09/06 01:41:37PM	ffc9432c7956b9f7d5cf69a55ba0d46
13 PriestHolmes2.jpg	139,562	05/09/06 01:47:56PM	15c21a2519b736658bb9f712879173e
14 roaf_w_w.jpg	137,958	05/09/06 01:41:06PM	2b1664585edd985bc302dcd3a785e1a5
15 shields_w_w.jpg	167,986	05/09/06 01:41:18PM	a65e3180cd73c4231a8be68f543e767e

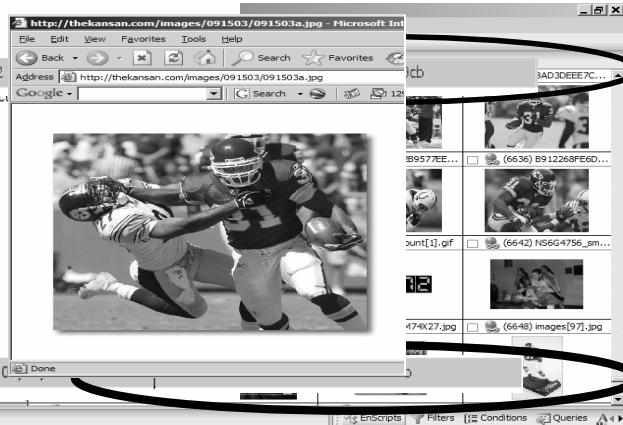
Internet Artifacts

Name 091503a.jpg
File Created 05/09/06 01:42:09PM
Last Accessed 05/10/06 02:47:05PM
Last Written 05/09/06 01:42:04PM
Disk Index Status 40,204,536

35021 091503a.jpg 117,792



35022 091503a[1].jpg 117,792



URL: http://thekansan.com/images/091503/091503a.jpg
Host: thekansan.com
Cached Date: 05/09/06 01:42:07PM
Cache Path: S1_R1_Q1_1\C\Documents and Settings\Shawn\Local Settings\Temporary Internet Files\Content.IE5\T9PI50I7\091503a

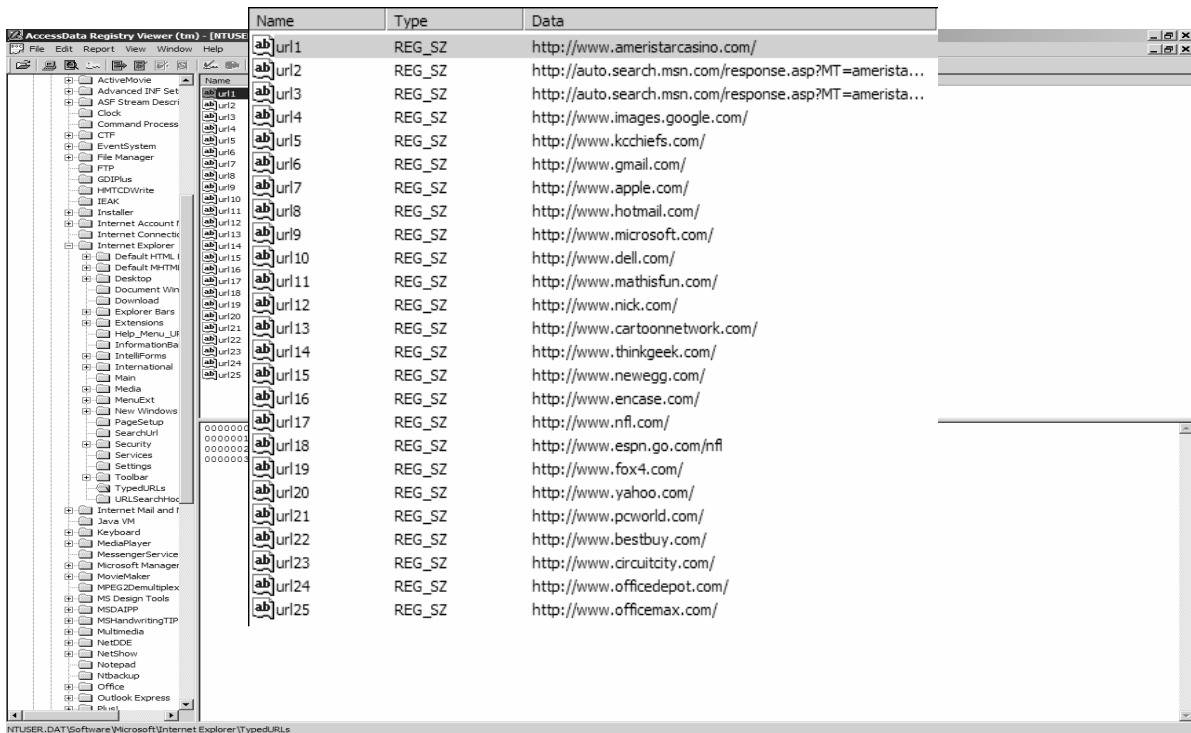
Picture



PDC Presentation[S1_R1_Q1_1\C\Documents and Settings\Shawn\Local Settings\Temporary Internet Files\Content.IE5\T9PI50I7\091503a

The MD5 hash for the picture located in the temporary internet files matches that of the one located in the “user created” folder. This indicates that it is the same file and now we know where the picture came from. The picture was saved by the computer user after it was viewed over the internet.

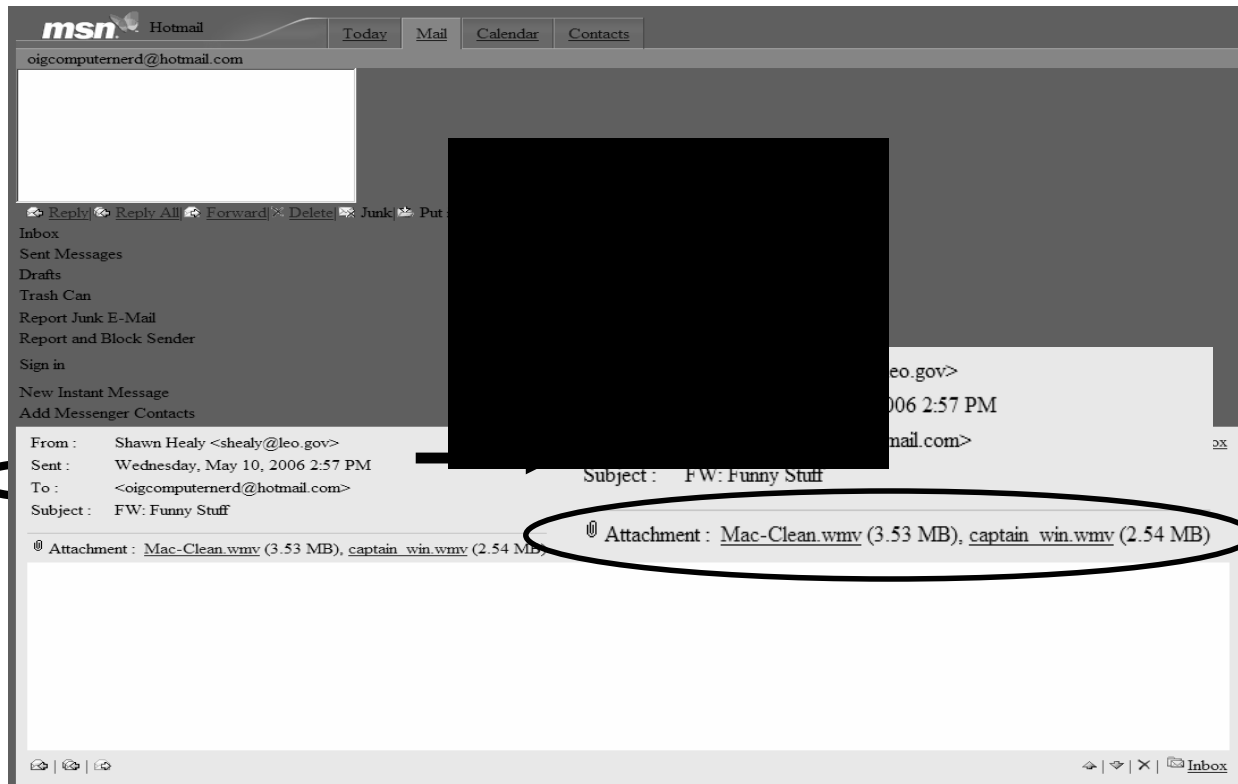
Typed URL Entries



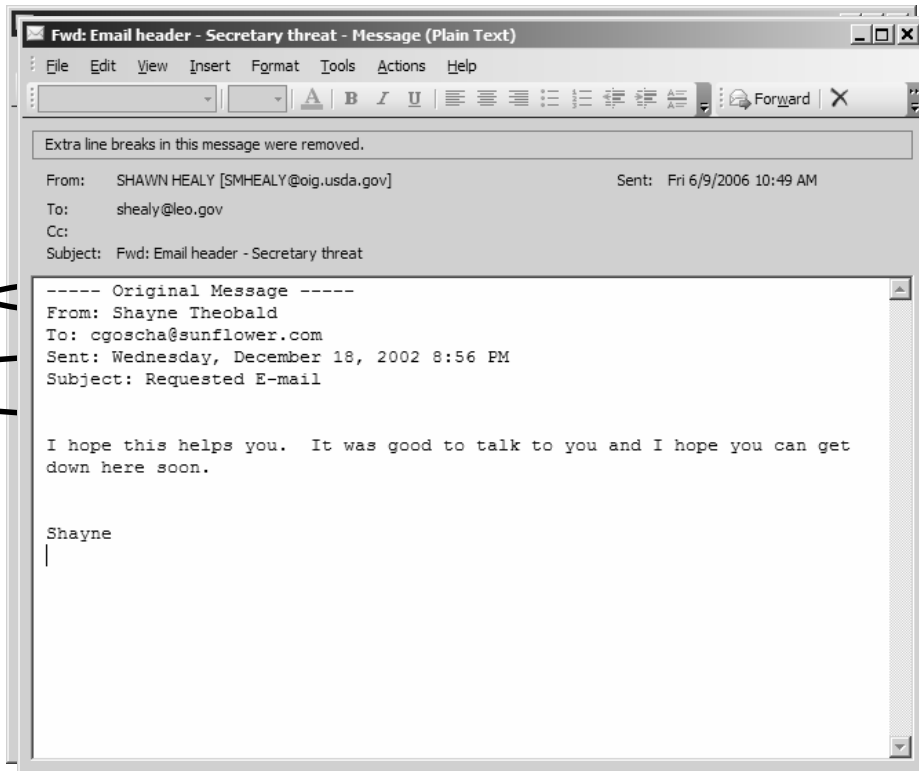
The screenshot shows the AccessData Registry Viewer interface. On the left is a tree view of the registry structure, with 'TypedURLs' selected under 'Internet Explorer'. The main pane displays a table of registry entries. The table has three columns: Name, Type, and Data. The entries are numbered from url1 to url25, all of type REG_SZ, and contain various web addresses.

Name	Type	Data
ab\url1	REG_SZ	http://www.ameristarcasino.com/
ab\url2	REG_SZ	http://auto.search.msn.com/response.asp?MT=amerista...
ab\url3	REG_SZ	http://auto.search.msn.com/response.asp?MT=amerista...
ab\url4	REG_SZ	http://www.images.google.com/
ab\url5	REG_SZ	http://www.kcchiefs.com/
ab\url6	REG_SZ	http://www.gmail.com/
ab\url7	REG_SZ	http://www.apple.com/
ab\url8	REG_SZ	http://www.hotmail.com/
ab\url9	REG_SZ	http://www.microsoft.com/
ab\url10	REG_SZ	http://www.dell.com/
ab\url11	REG_SZ	http://www.mathisfun.com/
ab\url12	REG_SZ	http://www.nick.com/
ab\url13	REG_SZ	http://www.cartoonnetwork.com/
ab\url14	REG_SZ	http://www.thinkgeek.com/
ab\url15	REG_SZ	http://www.newegg.com/
ab\url16	REG_SZ	http://www.encase.com/
ab\url17	REG_SZ	http://www.nfi.com/
ab\url18	REG_SZ	http://www.espn.go.com/nfi
ab\url19	REG_SZ	http://www.fox4.com/
ab\url20	REG_SZ	http://www.yahoo.com/
ab\url21	REG_SZ	http://www.pcwORLD.com/
ab\url22	REG_SZ	http://www.bestbuy.com/
ab\url23	REG_SZ	http://www.circuitcity.com/
ab\url24	REG_SZ	http://www.officedepot.com/
ab\url25	REG_SZ	http://www.officemax.com/

Web Based Email: Analysis and Recovery



Email: Tracing it Back



Other Potentially Important Information

The screenshot shows the AccessData Registry Viewer (tm) - [NTUSER.DAT] application. The left pane displays a tree view of registry keys, including:

- NetShow
- Notepad
- Ntbackup
- Office
- Outlook Express
- PhotoUploadControl
- Plus!
- Protected Storage System Provider
- S-1-5-21-2052111302-1383384898-1060284298-1003
 - IdentityMgr
 - InfoDelivery
 - Internet Explorer
 - Internet Explorer
 - https://bankcardsonline.commercebank.com/C
 - https://bankcardsonline.commercebank.com/C
 - https://secure.newegg.com/NewVersion/MyAc
 - https://secure.newegg.com/NewVersion/MyAc
 - http
 - q:StringData :counts/ServiceLogin:StringData
 - q:StringIndex :counts/ServiceLogin:StringIndex

The right pane shows a table with columns: Name, Type, and Data. The selected item is:

Name	Type	Data
Item Data	REG_MULTI_SZ	Wed May 10 18:50:15 2006 ---- "WDCOCIOFP03" Wed M...

A dialog box titled "Multiple String Values" is open, displaying the following data:

Value Name:	Data:
Item Data	Wed May 10 18:50:15 2006 ---- "WDCOCIOFP03"
	Wed May 10 18:50:24 2006 ---- "WDCOCIOFP"
	Thu May 11 12:44:26 2006 ---- chiefs
	Thu May 11 12:44:54 2006 ---- kcchiefs

The dialog box has a "Close" button at the bottom.

Did We Miss Something?

AccessData Registry Viewer (tm) - [system]

Name	Type	Data
DeviceDesc	REG_SZ	USB Mass Storage Device
LocationInformation	REG_SZ	JUMPRIVE PRO
Capabilities	REG_DWORD	0x0000014 (20)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	USB\Wid_05dc&Pid_a420&Rev_3000 USB\Wid_05dc&Pid_a420
CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
DeviceDesc	REG_SZ	USB Human Interface Device
LocationInformation	REG_SZ	External HDD
Capabilities	REG_DWORD	0x00000084 (132)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	USB\Wid_1058&Pid_0401&Rev_0412&MI_01 USB\Wid_1058&Pid_0401&MI_01
CompatibleIDs	REG_MULTI_SZ	USB\Class_03&SubClass_00&Prot_00 USB\Class_03&SubClass_00 USB\Class_03
ClassGUID	REG_SZ	{745A17A0-74D3-11D0-B6FE-00A0C90F57DA} JSB\COM..
Class	REG_SZ	HIDClass
Driver	REG_SZ	{745A17A0-74D3-11D0-B6FE-00A0C90F57DA}\0006
Mfg	REG_SZ	(Standard system devices)
Service	REG_SZ	HidUsb
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentIdPrefix	REG_SZ	7&1f947d47&0

Key Properties

Last Written Time: 5/9/2006 18:56:28 UTC

system\ControlSet001\Enum\USB\Wid_05dc&Pid_a420\35A3FB10172108281104 Offset: 0