Case Name:	Hunter XP	**Case No:**	001	**Case Sub Date:**	11/01/2024

1.

Forensic Examiner: Accreditation, Qualifications, and Training.

I, Sahifa Syed, am a first-year student at the University of the West of England, studying Cyber Security and Digital Forensics. This program has enabled me to gain a comprehensive understanding of the principles and practices involved in both cyber security and digital forensics. The curriculum covers a wide range of subjects that include computer crime and digital evidence, programming in C++ as well as introduction to databases.

By choosing this course I got the opportunity to actively participate in investigations (such as these i.e. HunterXP) , which gives me valuable hands-on experience in the field of digital forensics. This practical approach allows me to not only develop and expand my critical thinking, problem-solving, and analytical skills, but also to gain a deeper understanding of how these skills are applied in real-life scenarios.

This gives me the chance to work with different types of digital devices and explore various forensic tools and techniques. This exposure is crucial in preparing me for a successful career in the field of cyber security and digital forensics.

1.1 Evidence Media AND Forensic Tools

I, Sahifa Syed, received an evidence file in the.E01 (EnCase Evidence format) format on October 23, 2023. My investigation's aim was to look for any indications of activity that may be deemed as that going against the regulations with regards to the image. The image is a forensic duplicate of a digital device, which will also be called 'The computer' during the course of this investigation.

I made use of two forensic tools namely: Encase (Version 7.12.01) and Autopsy (Version 4.21.0). Encase assisted me with extensively viewing, analysing and extracting files , while Autopsy provided an alternative approach to verify the information provided. The combination of these tools not only facilitated a thorough analysis but also provided valuable insights that ultimately played a pivotal role in the case, resulting in a successful discovery and outcome of potential evidence.

1.2 Evidence Summary

On October 23, 2021, at 10:00 HRS, I processed the evidence file that was provided into EnCase and carried out a 'Hash verification' of the file to begin my investigation. This process was completed to make sure that the contents within evidence file was protected and it remains unchanged throughout the investigation. The hashes are shown in the **Fig. 1**. To view the hash verification on the forensic tools *encase* and *autopsy* , please refer to **Appendix 1**.

Verification hashes	
MD5	**dfcfe9ab9a60c6ad4a314656b687226b**
MD5 verification hash	**dfcfe9ab9a60c6ad4a314656b687226b**

Fig.1

2. Profiling The System

In order to determine what activity has taken place on the computer, I had to “profile” the computer. This process consists of gathering system information that has been mostly kept in the Operating System's (OS) main database, which is known as the "Registry". The registry saves the user settings and provides key information about the computer in use. It is a vital component to look into as it provides a variety of information during the course of this investigation.

2.1 Operating System And Timeline

The Operating System (OS) is the software program that allows a user to interact with the computer. It is used to run software applications and save files to the device on which it is installed. By utilizing EnCase's evidence processing function and through the system info parser, I gathered information about the OS. The information in **Fig.2** displays the data recovered from the **operating system’s service artifacts and time zone information registry keys,** refer to **Appendix 2** for provenance of this information. It was discovered that the operating system was installed on an NTFS file system, this information was recorded as it is significant for discussing dates and times.

Operating system information (System Artefacts)	
Product name	Microsoft Windows XP
Product ID	55277- 005-6418583-21673
Current Version	5.1
Registered Owner	PC User
Registered Organization	PC User Company
Install Date	Thu, 28 Feb 2002 22:02:39 GMT
Shutdown Time	Tue, 04 Jun 2002 22:58:42 GMT

Fig.2

The last file written to on the computer was on **28/02/2002 at 22:02:39 GMT.** This gives a timeline of **04/06/2002 and 22:58:42** . It is worth mentioning that these dates and times may not be entirely reliable, as they can be easily manipulated either intentionally or due to errors.

2.2 Time Zone Information

As mentioned in section 2.1, the operating system was found to be installed on an NTFS file system. Due to this, all file dates and times are stored in the Central Standard Time (CST) format. Using Encase, I extracted and analysed the registry files, which contain user settings and computer configurations. The 'controlset001' file found within the registry contained the computer's time zone information.

After locating this information, I made necessary adjustments to the evidence processors in both Encase and Autopsy to align with the information found in the registry of the imaged hard disk. This was done to ensure that all the dates and times were successfully converted to the local time of the machine, applying the necessary modifications based on the CST values. (refer to **Appendix 3** below)

2.3 User Account Info

Upon investigating the OS was found to hold the following user accounts, listed in **Fig.3**. A user account is an identity created for a person in a computer or a computing system**.** This data was obtained with the aid of the system info parser in the user account records section.

User Accounting Name	Built – In (Yes or No)	Last Log on
Administrator	Yes, Built -in account for administering the computer/domain	-
Bob Hunter	No	04/06/02 18:01:64
Guest	Yes, Built -in account for administering the computer/domain	03/06/02 11:49:37

Fig.3

The information above was recovered from system info parser. For detailed information on the source and credibility of this data, including the acquisition and processing methods, please refer to **Appendix 4**. It provides brief documentation and transparency regarding the user accounts' information.

2.4 Attached Devices

I utilized encase to determine which devices had been attached to the computer itself. I examined the 'USB records tab' with the aid of the system info parser, which revealed the presence of USB drives under the Hunter XP section. This USB drive was identified as external drives connected to the computer. See **Fig.4** and refer to **Appendix 5** below.

Name	Serial Number	User Account	Last Connected Date	Last Connected Time
Netac OnlyDisk	7&1042c72&0	Bob Hunter	03/06/02	15:05:15

Fig.4

2.5 Keyword Search

During the course of this investigation using Encase, I ran specific keyword searches relevant to the case by indexing the evidence files, processing it and then examining the end results. The outcome of these selected keyword searches proved to be highly informative and pivotal in progressing forward in the investigation as they provided information that could be seen as potential evidence. The key information of the keyword search was found and gathered from the *'system's keyword search records'* which is under the *'system info parser records'*. Please refer to **Appendix 6** to view the above keywords mentioned. This will give a thorough explanation of the context and search strategy used whilst investigating the case as well as the reasoning behind the choice of particular keywords.

2.6 Internet And Email Activity

Using Encase, I managed to locate and discover a various range of files that consisted of emails (local and web-based) as well as internet records which consists of internet history, favourites etc. This in-depth search and analysis of the files carried out within encase revealed a range of activities related to stalking. The case-relevant files were selected to be bookmarked, as they were important to the case. Refer to **Fig.5 and Fig.6** for the internet files and email activity recorded. For a more detailed understanding of these findings, see **Appendix 7** below. This information is also present in the *SS2: evidence report* which is a bookmark collection of potential evidence.

Bookmarks Name	Internet Typed URLs
NTUSER.DAT	www.thestalkershomepage.com
Christina and Sabrina	http://www.guidancesw.com/chrisina_sabrina.htm
The StalkingWebsite	http://www.glr.com./stalk.html

Fig.5

Bookmarks	Email Subject
Attachments found related to stalking activity	Web Site
Notable page	Re: Web Page on Christina

Fig.6

2.7 File Carving

I was able to locate and examine more relevant evidence for the case by using the data carving process. Data carving is a useful method that enables the retrieval of files that cannot be indexed by the file system. This includes files that have been erased or hidden and are stored in unallocated spaces. The files found within the data carving process were emails sent from the computer to the parent of the individual. These emails stood out in particular because they contained notable subjects and had repeatedly used the word 'daughter' in them. Referring to **Appendix 8 below**, the repeated use of the term in the email emphasizes its relevance and importance to the case. It also provides valuable information about the different types of relationships and the various methods of communications that are taking place.

2.8 Recycle Bin Content Analysis

To analyse the recycle bin content I used the Evidence Processor within EnCase to identify and view .LNK files. I examined and saved the relevant files name, location (path)and deleted dates (see **Fig.7**). I checked the integrity of the Recycle Bin files and found that no bypass or changes were made, which ensured the integrity of the Recycle Bin.

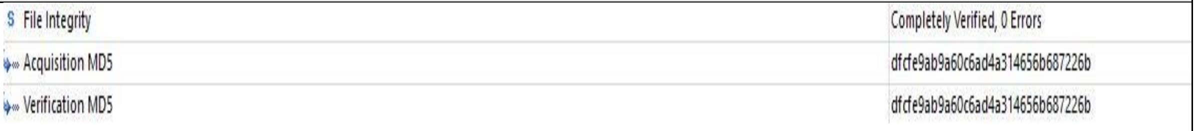
File Name	Original Path	Deleted Date
Sabrina Dewercs	F:\Documents and Setting\Bob Hunter\My Documents\My Pictures\Hunter Pics\Sabrina Dewercs	05/06/02 1:49:16
102-0283_IMG.JPG	F:\Document and Setting\ Bob Hunter\My Documents\My Pictures\Hunter Pics\Christina Detsiwt\102-0283	05/06/02 1:49:16
Thumbs.db	F:\Document and Setting\ Bob Hunter\My Documents\My Pictures\Hunter Pics\Christina Detsiwt\Thumbs.db	05/06/02 1:50:06

Fig.7

Evidence Appendix

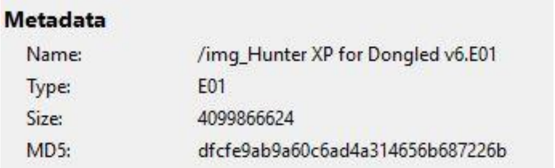
The Evidence Appendix below displays a range of images that serve as evidence I have collected for the hunter XP case mentioned above. These images provide visual documentation/depiction that supports the findings and claims presented in the preceding text. By including these images in the appendix, I aim to offer a thorough and clear representation of the evidence gathered during the investigation, allowing the readers to have a visual reference and further understand the specifics and context of the case itself.

Appendix 1.1 – Forensic Tool 1: Encase



File Integrity	Completely Verified, 0 Errors
Acquisition MD5	dfcfe9ab9a60c6ad4a314656b687226b
Verification MD5	dfcfe9ab9a60c6ad4a314656b687226b

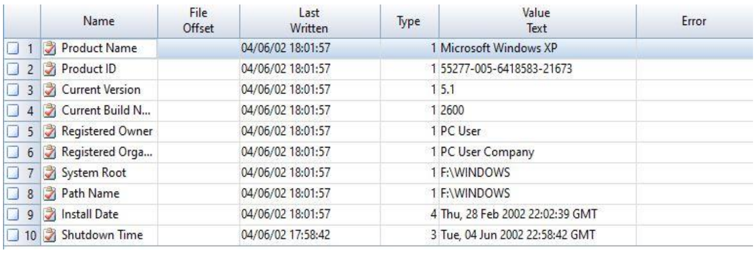
Appendix 1.2 – Forensic Tool 2: Autopsy



Metadata

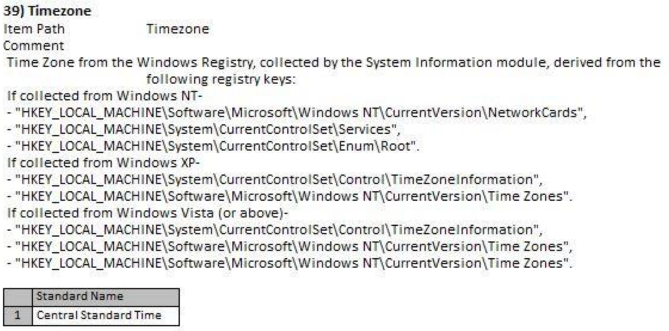
Name:	/img_Hunter XP for Dongled v6.E01
Type:	E01
Size:	4099866624
MD5:	dfcfe9ab9a60c6ad4a314656b687226b

Appendix 2 – Operating system information (System Artefacts) : Encase



	Name	File Offset	Last Written	Type	Value Text	Error
□ 1	Product Name		04/06/02 18:01:57	1	Microsoft Windows XP	
□ 2	Product ID		04/06/02 18:01:57	1	55277-005-6418583-21673	
□ 3	Current Version		04/06/02 18:01:57	1	5.1	
□ 4	Current Build N...		04/06/02 18:01:57	1	2600	
□ 5	Registered Owner		04/06/02 18:01:57	1	PC User	
□ 6	Registered Orga...		04/06/02 18:01:57	1	PC User Company	
□ 7	System Root		04/06/02 18:01:57	1	F:\WINDOWS	
□ 8	Path Name		04/06/02 18:01:57	1	F:\WINDOWS	
□ 9	Install Date		04/06/02 18:01:57	4	Thu, 28 Feb 2002 22:02:39 GMT	
□ 10	Shutdown Time		04/06/02 17:58:42	3	Tue, 04 Jun 2002 22:58:42 GMT	

Appendix 3 – Time Zone Information : Encase



39) Timezone

Item Path Timezone

Comment

Time Zone from the Windows Registry, collected by the System Information module, derived from the following registry keys:

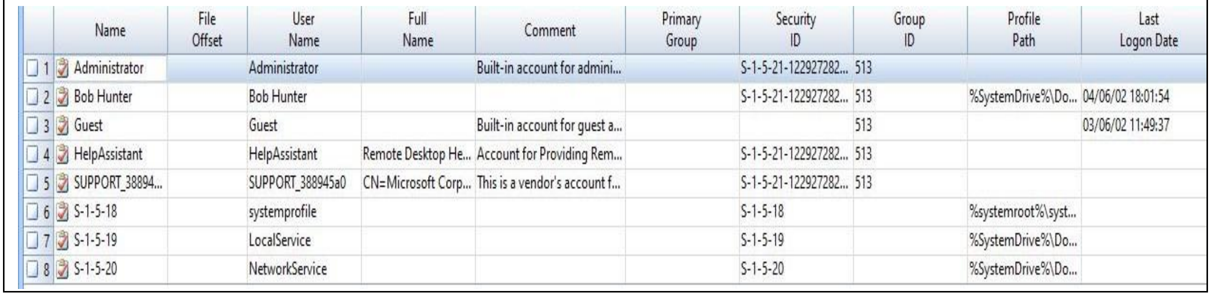
If collected from Windows NT-
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\NetworkCards",
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services",
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\Root".

If collected from Windows XP-
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation",
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones".

If collected from Windows Vista (or above)-
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation",
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones",
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones".

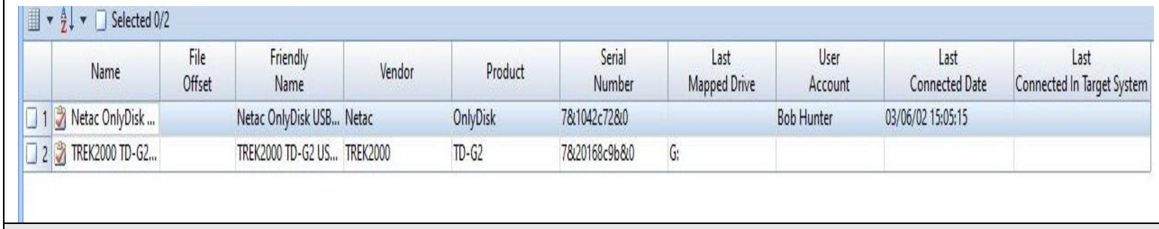
	Standard Name
1	Central Standard Time

Appendix 4 – User Accounts Information : Encase



	Name	File Offset	User Name	Full Name	Comment	Primary Group	Security ID	Group ID	Profile Path	Last Logon Date
□ 1	Administrator		Administrator		Built-in account for admini...		S-1-5-21-122927282...	513		
□ 2	Bob Hunter		Bob Hunter				S-1-5-21-122927282...	513	%SystemDrive%\Do...	04/06/02 18:01:54
□ 3	Guest		Guest		Built-in account for guest a...			513		03/06/02 11:49:37
□ 4	HelpAssistant		HelpAssistant	Remote Desktop He...	Account for Providing Rem...		S-1-5-21-122927282...	513		
□ 5	SUPPORT_38894...		SUPPORT_388945a0	CN=Microsoft Corp...	This is a vendor's account f...		S-1-5-21-122927282...	513		
□ 6	S-1-5-18		systemprofile				S-1-5-18		%systemroot%\syst...	
□ 7	S-1-5-19		LocalService				S-1-5-19		%SystemDrive%\Do...	
□ 8	S-1-5-20		NetworkService				S-1-5-20		%SystemDrive%\Do...	

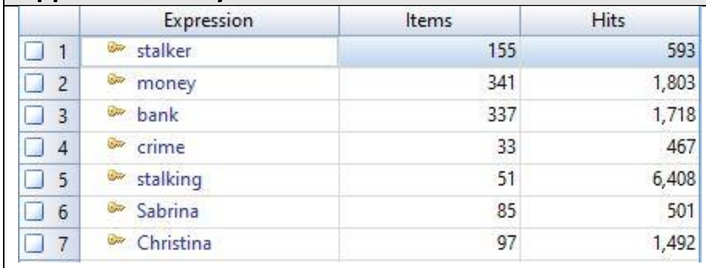
Appendix 5 – Attached Drives : Encase



□ Selected 0/2

	Name	File Offset	Friendly Name	Vendor	Product	Serial Number	Last Mapped Drive	User Account	Last Connected Date	Last Connected In Target System
□ 1	Netac OnlyDisk ...		Netac OnlyDisk USB...	Netac	OnlyDisk	7&1042c72&0		Bob Hunter	03/06/02 15:05:15	
□ 2	TREK2000 TD-G2...		TREK2000 TD-G2 US...	TREK2000	TD-G2	7&20168c9b&0	G:			

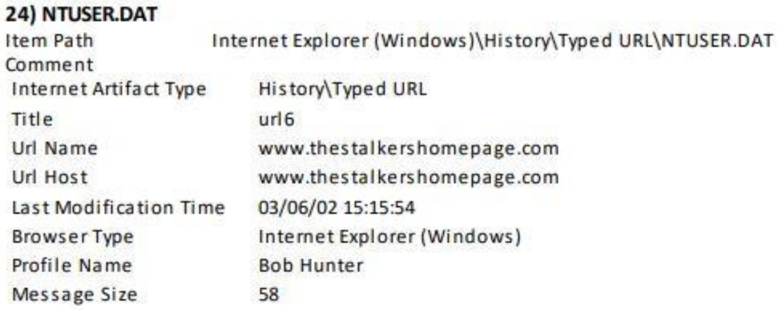
Appendix 6 – Keyword Search : Encase



	Expression	Items	Hits
□ 1	stalker	155	593
□ 2	money	341	1,803
□ 3	bank	337	1,718
□ 4	crime	33	467
□ 5	stalking	51	6,408
□ 6	Sabrina	85	501
□ 7	Christina	97	1,492

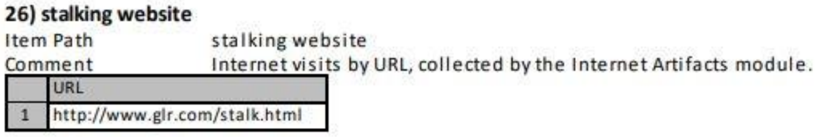
Appendix 7 – Internet and Email Activity : Encase

Internet Activity Bookmarks : Using Encase



24) NTUSER.DAT

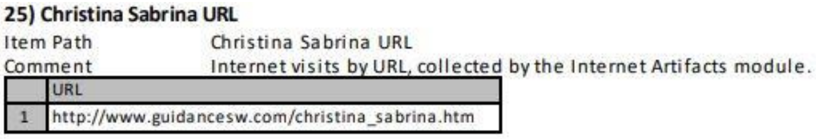
Item Path	Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT
Comment	
Internet Artifact Type	History\Typed URL
Title	url6
Url Name	www.thestalkershomepage.com
Url Host	www.thestalkershomepage.com
Last Modification Time	03/06/02 15:15:54
Browser Type	Internet Explorer (Windows)
Profile Name	Bob Hunter
Message Size	58



26) stalking website

Item Path	stalking website
Comment	Internet visits by URL, collected by the Internet Artifacts module.

	URL
1	http://www.glr.com/stalk.html

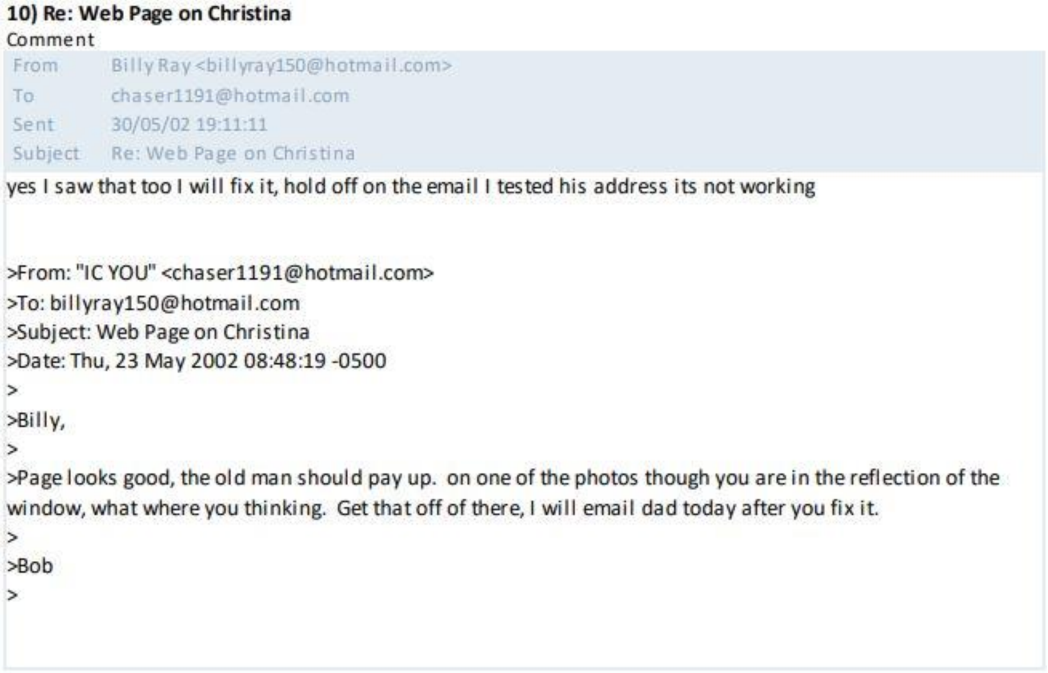


25) Christina Sabrina URL

Item Path	Christina Sabrina URL
Comment	Internet visits by URL, collected by the Internet Artifacts module.

	URL
1	http://www.guidancesw.com/christina_sabrina.htm

Email Activity Bookmarks : Using Encase



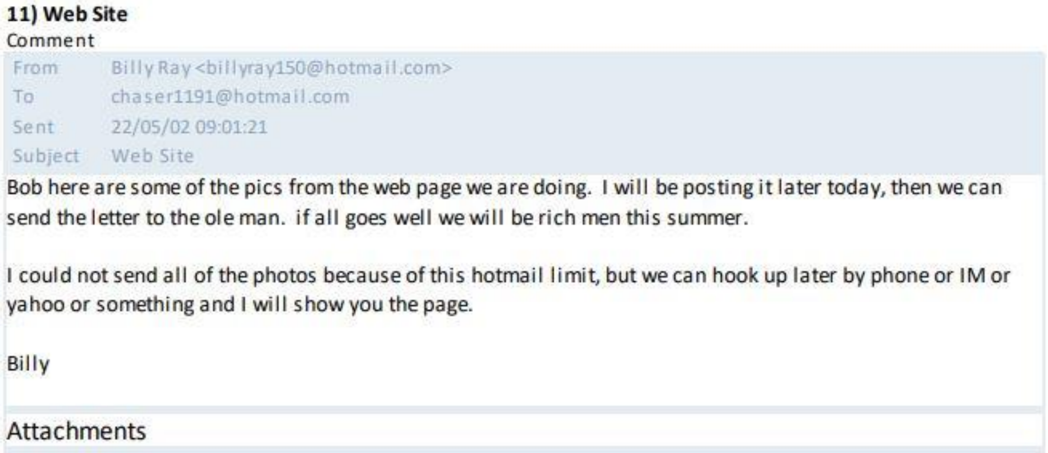
10) Re: Web Page on Christina

Comment

From	Billy Ray <billyray150@hotmail.com>
To	chaser1191@hotmail.com
Sent	30/05/02 19:11:11
Subject	Re: Web Page on Christina

yes I saw that too I will fix it, hold off on the email I tested his address its not working

>From: "IC YOU" <chaser1191@hotmail.com>
>To: billyray150@hotmail.com
>Subject: Web Page on Christina
>Date: Thu, 23 May 2002 08:48:19 -0500
>
>Billy,
>
>Page looks good, the old man should pay up. on one of the photos though you are in the reflection of the window, what where you thinking. Get that off of there, I will email dad today after you fix it.
>
>Bob
>



11) Web Site

Comment

From	Billy Ray <billyray150@hotmail.com>
To	chaser1191@hotmail.com
Sent	22/05/02 09:01:21
Subject	Web Site

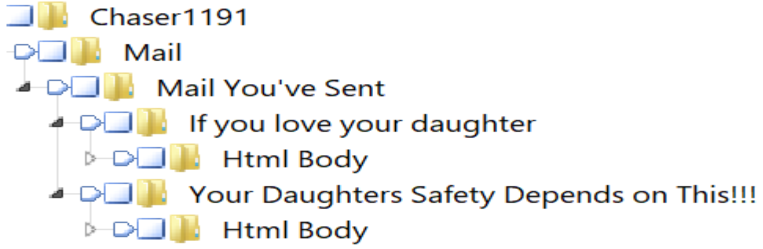
Bob here are some of the pics from the web page we are doing. I will be posting it later today, then we can send the letter to the ole man. if all goes well we will be rich men this summer.

I could not send all of the photos because of this hotmail limit, but we can hook up later by phone or IM or yahoo or something and I will show you the page.

Billy

Attachments

Appendix 8 – File Carving : Encase



- Chaser1191
  - Mail
    - Mail You've Sent
      - If you love your daughter
        - Html Body
      - Your Daughters Safety Depends on This!!!
        - Html Body