

What's the username/password for the telnet/ftp account?

Username:gnome

Password:gnome123

NewMiner 2.2

File Tools Help

Select a network adapter in the list —

Hosts (168) Files (157) Images (117) Messages (2) Credentials (60) Sessions (278) DNS Parameters (38328) Keywords Anomalies

☒ Show Cookies ☒ Show NTLM challenge-response ☐ Mask Passwords

Client	Server	Protocol	Username	Password	Valid to	Login timestamp
137.30.122.253 (Windows)	137.30.120.40 (Sofatec)	FTP	gromote		gromote.123	Unknown
137.30.122.253 (Windows)	64.233.167.104 [www.google.com]	HTTP Cookie	PREF=ID=269e53562e59c3c5 TM=1082665136 LM=108	N/A	Unknown	2004-04-26 17:21:45 UTC+05
137.30.122.253 (Windows)	207.68.173.245 [www.hotmail.com] (Windows)	HTTP Cookie	SITESERVERID=0-d0ee5efaccd4faae71819d9f05478	N/A	Unknown	2004-04-26 17:18:47 UTC+05
137.30.122.253 (Windows)	65.54.225.254 [ognnet.passport.net] (Windows)	HTTP Cookie	MSPPre-hugehnholver@hotmail.com	N/A	Unknown	2004-04-26 17:18:47 UTC+05
137.30.122.253 (Windows)	64.4.328.245 [ognnet.passport.net] (Windows)	HTTP Cookie	MSPFlow=4-1080179203ba-1ba2c	N/A	Unknown	2004-04-26 17:18:47 UTC+05
137.30.122.253 (Windows)	65.54.226.255 [ognn.safepoint.net] (Windows)	HTTP Cookie	MSPFlow=4-1080179203ba-1ba2c	N/A	Unknown	2004-04-26 17:18:49 UTC+05
137.30.122.253 (Windows)	207.68.172.240 [ib.msn.com] (Windows)	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:05 UTC+05
137.30.122.253 (Windows)	207.68.172.240 [ib.msn.com]	HTTP Cookie	y=1; domain=.msn.com; path=/	N/A	Unknown	2004-04-26 17:18:50 UTC+05
137.30.122.253 (Windows)	64.4.33.7 [www.hotmail.mn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:07 UTC+05
137.30.122.253 (Windows)	64.4.33.7 [www.hotmail.mn.com]	HTTP Cookie	FIM-112dang12cEHY2icatabyley12c412ccokuter12cwv	N/A	Unknown	2004-04-26 17:19:07 UTC+05
137.30.122.253 (Windows)	64.4.325.250 by17dbay17html.msn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:07 UTC+05
137.30.122.253 (Windows)	64.4.325.250 by17dbay17html.msn.com]	HTTP Cookie	FIM-112dang12cEHY2icatabyley12c412ccokuter12cbv1	N/A	Unknown	2004-04-26 17:19:09 UTC+05
137.30.122.253 (Windows)	64.4.325.250 by17dbay17html.msn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:18 UTC+05
137.30.122.253 (Windows)	207.68.172.236 [ib.msn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:28 UTC+05
137.30.122.253 (Windows)	207.68.172.124 [ib.msn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:28 UTC+05
137.30.122.253 (Windows)	65.54.194.117 [ad.msn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:28 UTC+05
137.30.122.253 (Windows)	65.54.192.248 [popu.msn.com] (Windows)	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:19:28 UTC+05
137.30.122.253 (Windows)	64.4.325.250 by17dbay17html.msn.com]	HTTP Cookie	HMSO095-229uhghinlover140html%2ecommyWEB	N/A	Unknown	2004-04-26 17:23:21 UTC+05
137.30.122.253 (Windows)	64.4.325.250 by17dbay17html.msn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:23:32 UTC+05
137.30.122.253 (Windows)	64.4.325.250 by17dbay17html.msn.com]	HTTP Cookie	FIM-espressWed Dec 31 16:00:01 1969. domain=.msn.	N/A	Unknown	2004-04-26 17:23:32 UTC+05
137.30.122.253 (Windows)	65.54.226.247 [ognnet.passport.net] (Windows)	HTTP Cookie	MSPPre-hugehnholver@hotmail.com; BrowserTest-Succ.	N/A	Unknown	2004-04-26 17:23:32 UTC+05
137.30.122.253 (Windows)	65.54.226.247 [ognnet.passport.net] (Windows)	HTTP Cookie	MSPShVw=@@. domain=.passport.com;path=/version1	N/A	Unknown	2004-04-26 17:23:32 UTC+05
137.30.122.253 (Windows)	65.54.226.252 [ognn.passpoet.net] (Windows)	HTTP Cookie	MSPDom-espress-Thru.30-Oct-1980 16:00:00 GMT.dom.	N/A	Unknown	2004-04-26 17:23:34 UTC+05
137.30.122.253 (Windows)	65.54.230.240 [ognn.passpoet.net] (Windows)	HTTP Cookie	MSPPre-hugehnholver@hotmail.com; BrowserTest-Succ.	N/A	Unknown	2004-04-26 17:23:35 UTC+05
137.30.122.253 (Windows)	64.4.32.7 [www.hotmail.mn.com]	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:23:35 UTC+05
137.30.122.253 (Windows)	65.54.230.240 [ognn.passpoet.net] (Windows)	HTTP Cookie	MSPVw-espress-Thru.30-Oct-1980 16:00:00 GMT.domain.	N/A	Unknown	2004-04-26 17:23:35 UTC+05
137.30.122.253 (Windows)	64.4.32.7 [www.hotmail.mn.com]	HTTP Cookie	FIM-espress-Wed Dec 31 16:00:01 1969. domain=.msn.	N/A	Unknown	2004-04-26 17:23:35 UTC+05
137.30.122.253 (Windows)	207.68.171.245 [www.msn.com] (Windows)	HTTP Cookie	MC1+v-V3GUID=0e761e9f34650b4842c72ab1d3d52	N/A	Unknown	2004-04-26 17:23

What relevant file transfers appear in the network traces?

There are three file transfers for rhino images in the rhino log file.

NetworkMiner.LZ

FileToolsHelp

Select a network adapter in the list...

Hosts (168)Files (157)Images (117)Messages (2)Credentials (60)Sessions (278)DNSParameters (38828)KeywordsAnomalous

Filter keyword☐ Case sensitive☐ ExactPhraseAny columnClearApply

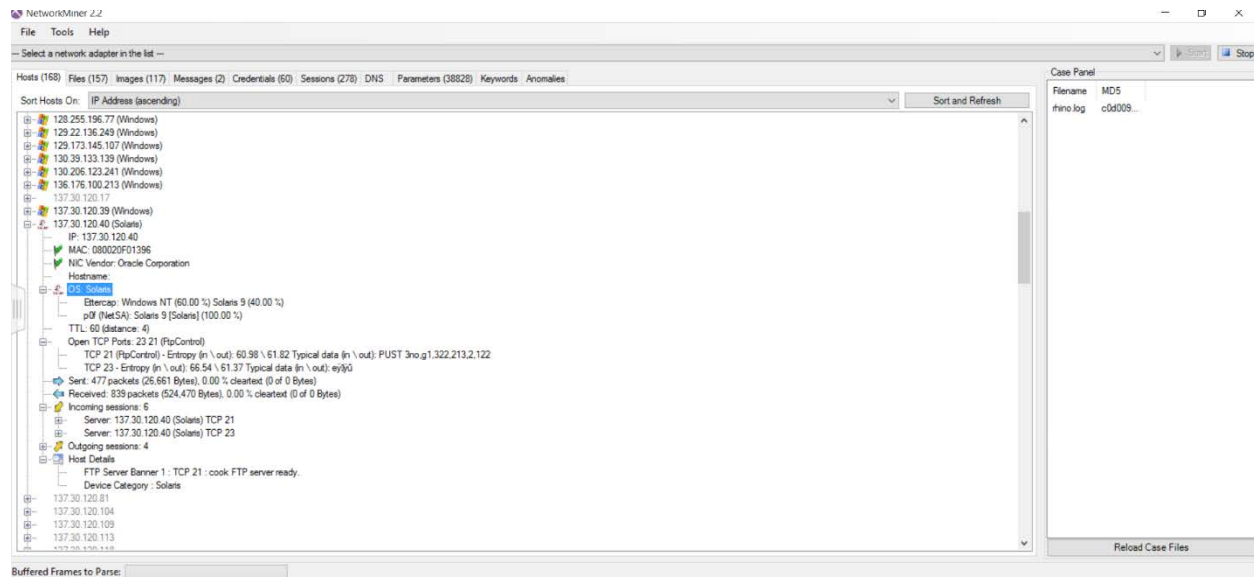
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed file path
4	index[1].html	html	2 934 B	64.233.167.104 [www.google.com]	TCP 80	137.30.122.253 (Windows)	TCP 1583	HttpGetNormal	2004-04-26 17:18:41 UTC-05	C:\Lab Files\NetworkMnre
16	index[2].html	html	236 B	207.68.173.245 [www.hotmail.com] (Windows)	TCP 80	137.30.122.253 (Windows)	TCP 1585	HttpGetNormal	2004-04-26 17:18:47 UTC-05	C:\Lab Files\NetworkMnre
27	login.asp.73DAF675[1].html	html	885 B	65.54.225.254 [login.passport.com] (Windows)	TCP 80	137.30.122.253 (Windows)	TCP 1587	HttpGetNormal	2004-04-26 17:18:47 UTC-05	C:\Lab Files\NetworkMnre
78	cbm.js.a5rh.D0AFCS7[2].js	js	8 751 B	207.68.172.240 [cb.man.com] (Windows)	TCP 80	137.30.122.253 (Windows)	TCP 1593	HttpGetNormal	2004-04-26 17:18:50 UTC-05	C:\Lab Files\NetworkMnre
109	login.passport.com[1].cer	cer	910 B	65.54.225.254 [login.passport.com] (Windows)	TCP 443	137.30.122.253 (Windows)	TCP 1594	TlsCertificate	2004-04-26 17:19:05 UTC-05	C:\Lab Files\NetworkMnre
148	hntome.127469CS[1].html	html	19 041 B	64.4.43.250 [17d.bay17.hotmail.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1598	HttpGetNormal	2004-04-26 17:19:09 UTC-05	C:\Lab Files\NetworkMnre
248	hotmal_908000006[1].css	css	3 267 B	64.4.43.250 [17d.bay17.hotmail.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1600	HttpGetNormal	2004-04-26 17:19:18 UTC-05	C:\Lab Files\NetworkMnre
274	helpcane_908000001[1].js	js	3 801 B	64.4.43.250 [17d.bay17.hotmail.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1602	HttpGetNormal	2004-04-26 17:19:25 UTC-05	C:\Lab Files\NetworkMnre
299	hotmal_90815000014[1].js	js	20 633 B	64.4.43.250 [17d.bay17.hotmail.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1605	HttpGetNormal	2004-04-26 17:19:27 UTC-05	C:\Lab Files\NetworkMnre
391	c.gf.C526B06[2].gif	gif	42 B	207.68.177.124 [h.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1615	HttpGetNormal	2004-04-26 17:19:28 UTC-05	C:\Lab Files\NetworkMnre
407	bpoupuprame.asp.23286AF0[1].html	html	218 B	65.54.192.248 [popup.man.com] (Windows)	TCP 80	137.30.122.253 (Windows)	TCP 1617	HttpGetNormal	2004-04-26 17:19:28 UTC-05	C:\Lab Files\NetworkMnre
404	ADSA0Cler31.dl.A6B0288[1].html	html	1 126 B	65.54.194.117 [ad.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1616	HttpGetNormal	2004-04-26 17:19:28 UTC-05	C:\Lab Files\NetworkMnre
475	bpoupup.asp.23286AF0[1].html	html	748 B	65.54.192.248 [popup.man.com] (Windows)	TCP 80	137.30.122.253 (Windows)	TCP 1623	HttpGetNormal	2004-04-26 17:19:29 UTC-05	C:\Lab Files\NetworkMnre
475	ADSA0Cler31.dl.F9AD8AE7[1].html	html	489 B	65.54.194.117 [ad.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1616	HttpGetNormal	2004-04-26 17:19:29 UTC-05	C:\Lab Files\NetworkMnre
1548	rhino[1].jpg	jpg	65 703 B	137.30.122.253 (Windows)	TCP 1657	137.30.120.40 (Solara)	TCP 20	FTP	2004-04-26 17:21:49 UTC-05	C:\Lab Files\NetworkMnre
1651	rhino[2].jpg	jpg	96 899 B	137.30.122.253 (Windows)	TCP 1660	137.30.120.40 (Solara)	TCP 20	FTP	2004-04-26 17:22:08 UTC-05	C:\Lab Files\NetworkMnre
1765	rhino[3].jpg	jpg	96 899 B	137.30.122.253 (Windows)	TCP 1662	137.30.120.40 (Solara)	TCP 20	FTP	2004-04-26 17:22:16 UTC-05	C:\Lab Files\NetworkMnre
2435	p.send[1].gif	gif	149 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1667	HttpGetNormal	2004-04-26 17:22:29 UTC-05	C:\Lab Files\NetworkMnre
2436	p.folder.draft[1].gif	gif	240 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1668	HttpGetNormal	2004-04-26 17:22:29 UTC-05	C:\Lab Files\NetworkMnre
2467	p.importance[1].gif	gif	160 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1672	HttpGetNormal	2004-04-26 17:22:30 UTC-05	C:\Lab Files\NetworkMnre
2468	p.attach[1].gif	gif	68 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1671	HttpGetNormal	2004-04-26 17:22:30 UTC-05	C:\Lab Files\NetworkMnre
2381	compose.B4399B8E[1].html	html	19 658 B	64.4.43.250 [17d.bay17.hotmail.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1664	HttpGetNormal	2004-04-26 17:22:28 UTC-05	C:\Lab Files\NetworkMnre
2493	p.downarrow[1].gif	gif	52 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1676	HttpGetNormal	2004-04-26 17:22:30 UTC-05	C:\Lab Files\NetworkMnre
2496	p.importance[1].gif	gif	171 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1677	HttpGetNormal	2004-04-26 17:22:30 UTC-05	C:\Lab Files\NetworkMnre
2499	c.gf.C526B16[2].gif	gif	42 B	207.68.177.124 [h.man.com]	TCP 80	137.30.122.253 (Windows)	TCP 1678	HttpGetNormal	2004-04-26 17:22:30 UTC-05	C:\Lab Files\NetworkMnre
2520	p.cancel[1].gif	gif	330 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1681	HttpGetNormal	2004-04-26 17:22:31 UTC-05	C:\Lab Files\NetworkMnre
2523	p.tool[1].gif	gif	168 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1682	HttpGetNormal	2004-04-26 17:22:31 UTC-05	C:\Lab Files\NetworkMnre
2542	p.attachfile[1].gif	gif	239 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1685	HttpGetNormal	2004-04-26 17:22:31 UTC-05	C:\Lab Files\NetworkMnre
2545	p.delete.d[1].gif	gif	306 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1686	HttpGetNormal	2004-04-26 17:22:31 UTC-05	C:\Lab Files\NetworkMnre
2625	p.attachfile[1].gif	gif	239 B	64.4.48.24 [64.4.48.24]	TCP 80	137.30.122.253 (Windows)	TCP 1685	HttpGetNormal	2004-04-26 17:22:31 UTC-05	C:\Lab Files\NetworkMnre

Case Panel
Filename MD5
rhino.jpg c06009...

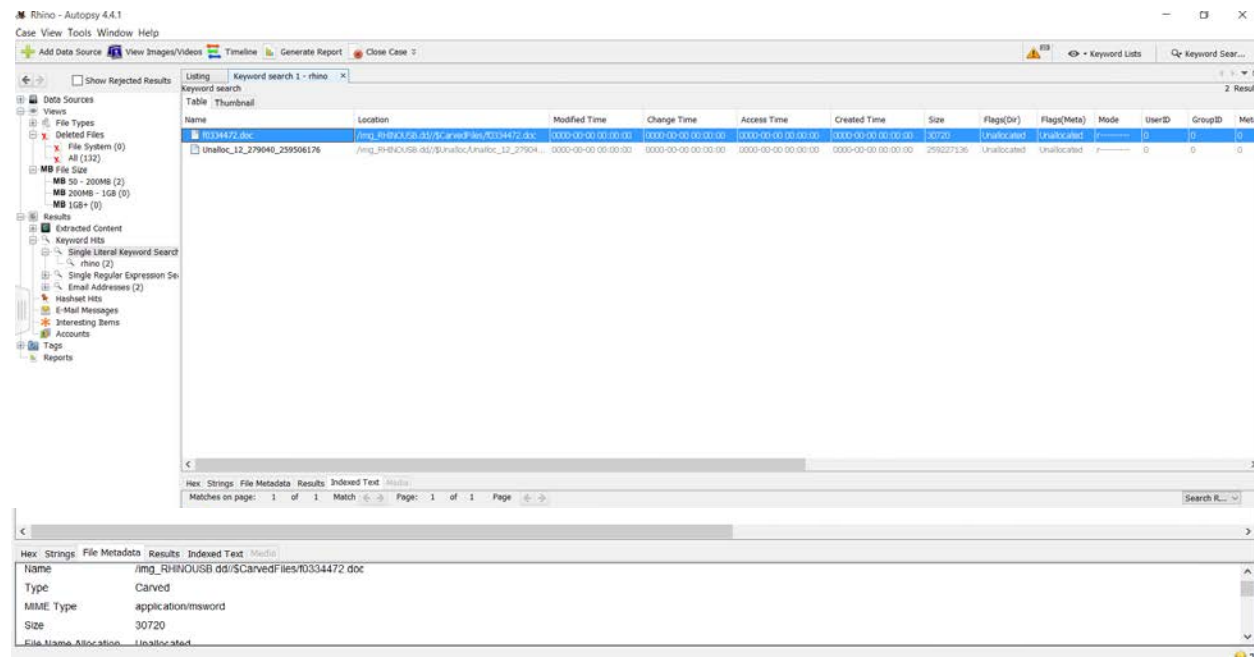
Relead Case Files

Buffered Frames to Parse

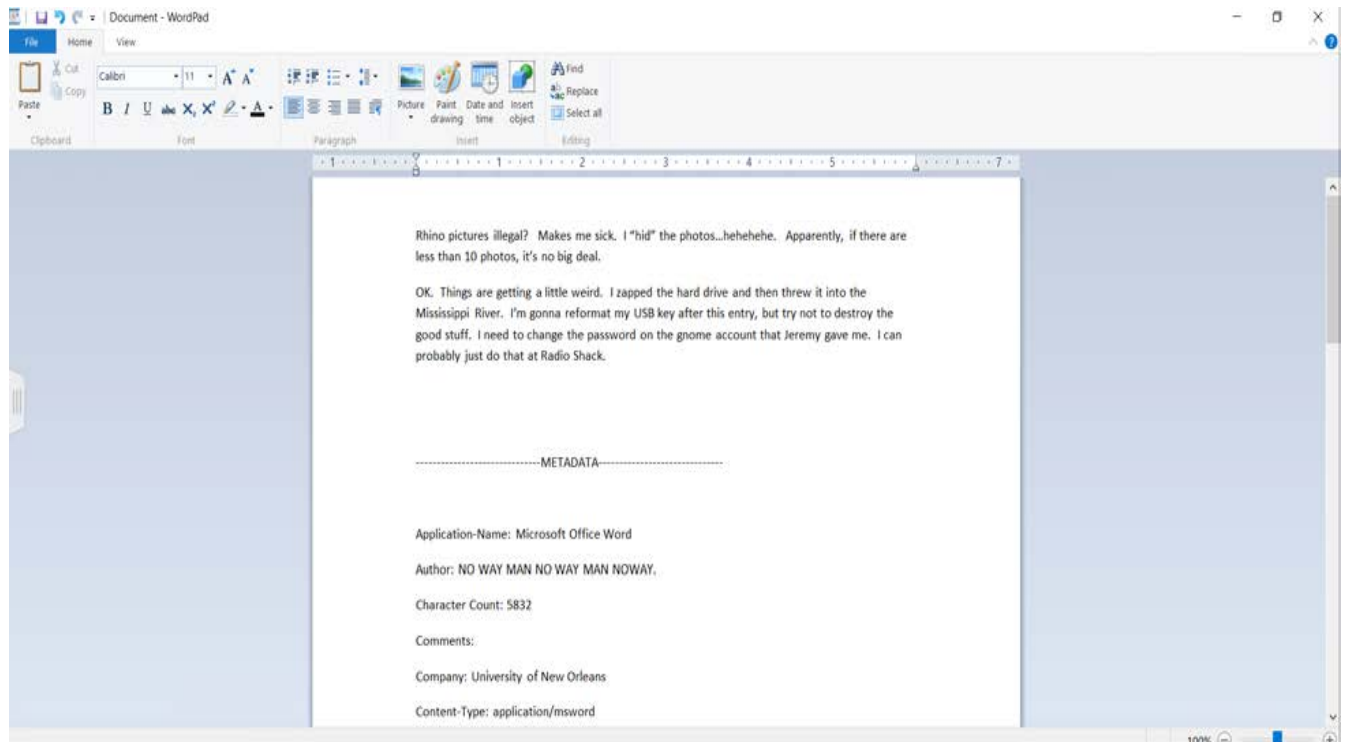
137.30.120.40 (Solaris) is the destination host for the rhino file's transfer.



I used Autopsy to run a rhino keyword search on the USB.
Below is the results from the search.



Below a screenshot of the text from the word document found in the hard drives unallocated space.



What happened to the hard drive in the computer? Where is it now?

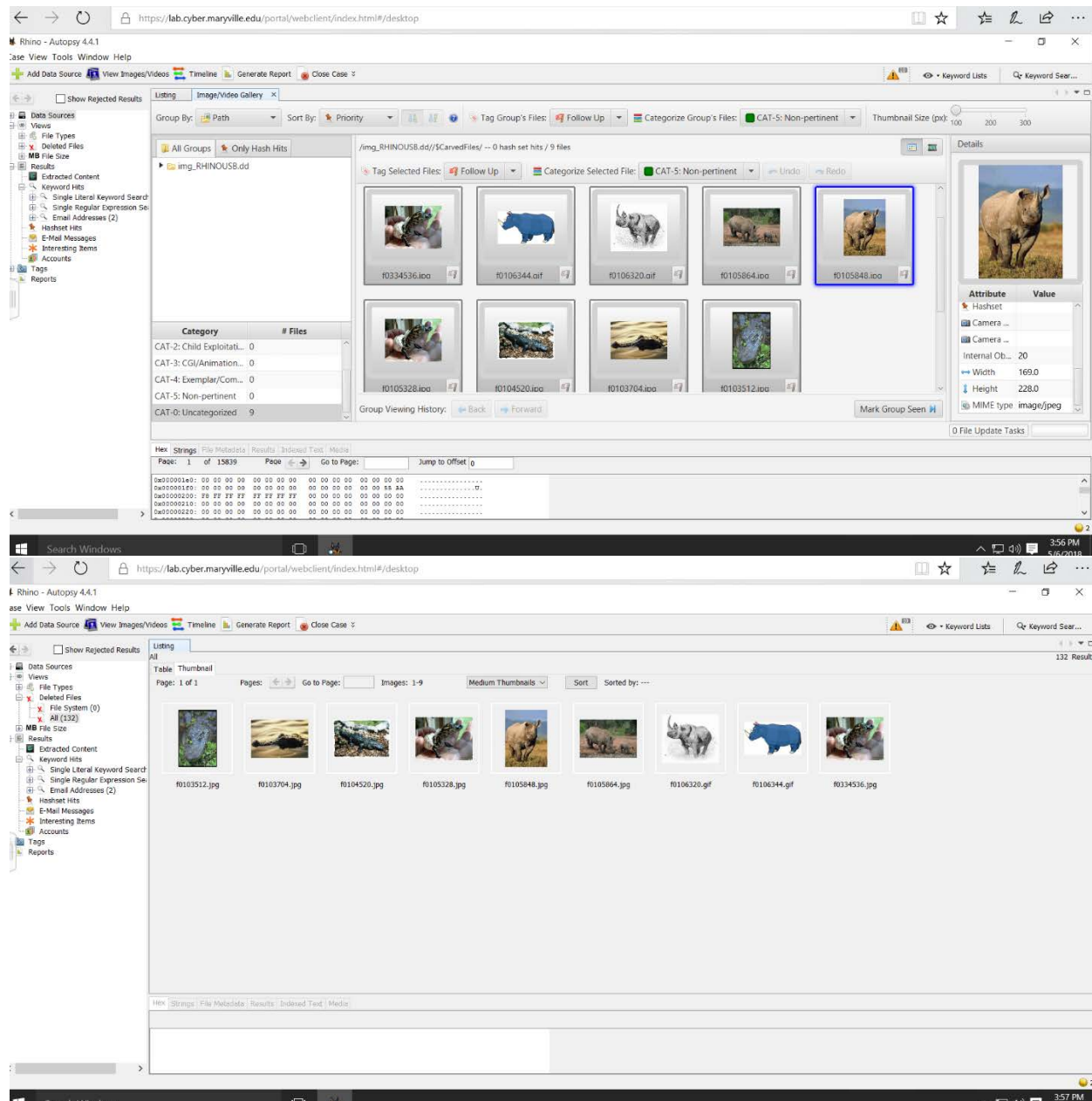
The hard drive was destroyed by the culprit and thrown into the Mississippi River.

What happened to the USB key?

The USB key was reformatted.

What is recoverable from the dd image of the USB key?

There are numerous pictures of rhino's in the deleted files.



Is there any evidence that connects the USB key and the network traces? If so, what?

In the network trace there is an email stating that the rhino pictures were uploaded to gnome account. In the network trace log there is a user name and password for the gnome account. Also on the USB key there is a word document detailing the destroying of the hard-drive, the reformatting of the usb key and also changing the password on the gnome account.