Module B8: File Recovery from Intercept Network Traffic Log.

Pre-requisite Knowledge and Skills:

1. Understand basic of internet/network communication

Learning Objectives

- 1. Understand the basic of internet communications.
- 2. Understand the risks of communication through internet.
- 3. Be exposed to methodology on communication interception and traffic log analysis.

Recommended Running Environment/Tools:

- 1. Windows OS
- 2. Wireshark
- 3. xvi32.exe (the xvi32 folder)

Material:

- 1. rhino.log
- 2. rhino2.log

Video Lecture:

1. Network File Recovery

Lab Assessment:

1. Network File Recovery Quiz

Acknowledgement:

The log files, rhino.log and rhino2.log, are obtained from DFRWS 2005 Rodeo Challenge, <u>https://www.dfrws.org/search</u>

Lab Instructions:

1. Scenario Description

You are chatting with your friends and transferred pictures by using a popular application (which uses ftp and http, a faked scenario). However, someone intercept your traffic by sniffing the communication signals and dumped into a few log files

- What you need to worry about?
- Can that person get the pictures you sent to your friends?
- How about login username and password?

<u>Tasks</u>

- Giving rhino.log and rhino2.log and wireshark tool
- Looking for password and user through FTP protocol
- Recover raw FTP transferred data (FTPData protocol, rhino.log)
 - Rhino1.jpg
- Recover http transferred data (rhino2.log, and xvi32.exe to edit)
 - Rhino4.jpg

2. Assessment

• Recover a rhino5.gif file from the http transferred data (rhino2.log, the file signature is GIF89a).

3. Step by Step Instructions

FTP Transmitted File Recovery

1. Load traffic log file into Wireshark for traffic analysis

📕 rhino.log	Sec. 18. 1					
<u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o	<u>Capture</u> <u>A</u> nalyze <u>S</u> ta	itistics Telephon <u>y W</u> irele	ess <u>T</u> ools <u>H</u> elp		
	۵ 🌡 🗈	। 🔀 🖸 । ९. 👄 🔿 🖻	i T 🞍 🗖 🗐 🔍 🤅	a, a, 🎹		
Apply a dis	play filter ·	<ctrl-></ctrl->				Expression +
No. Tir	ne	Source	Destination	Protocol	Length Info	*
10.	000000	137.30.122.253	64.233.167.104	TCP	62 1583 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	
2 0.	082001	64.233.167.104	137.30.122.253	TCP	60 80 → 1583 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460	
3 0.	082151	137.30.122.253	64.233.167.104	TCP	54 1583 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
4 0.	084413	137.30.122.253	64.233.167.104	HTTP	351 GET / HTTP/1.1	
5 0.	172955	64.233.167.104	137.30.122.253	TCP	1484 [TCP segment of a reassembled PDU]	
6 0.	318901	137.30.122.253	64.233.167.104	TCP	54 1583 → 80 [ACK] Seq=298 Ack=1431 Win=62810 Len=0	
7 0.	396683	64.233.167.104	137.30.122.253	TCP	272 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]	
8 0.						
9 0.	397383	64.233.167.104	137.30.122.253	TCP	1484 [TCP Out-Of-Order] 80 → 1583 [ACK] Seq=1431 Ack=298 Win=2920 Len=1430	
10 0.	397583	137.30.122.253	64.233.167.104	TCP	54 1583 → 80 [ACK] Seq=298 Ack=3079 Win=64240 Len=0	
11 4.	071502	158.94.89.167	137.30.120.113	TCP	62 3288 → 2745 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	
12 5.	377507	146.151.55.59	137.30.122.253	TCP	62 2358 → 2745 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	
_ 13 5.	831955	137.30.122.253	207.68.173.245	TCP	62 1585 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1	
14 6.	047759	207.68.173.245	137.30.122.253	TCP	62 80 → 1585 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 SACK_PERM=1	_
15 6.	047905	137.30.122.253	207.68.173.245	TCP	54 1585 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
16 6.	049725	137.30.122.253	207.68.173.245	HTTP	488 GET / HTTP/1.1	
17 6.	256202	207.68.173.245	137.30.122.253	TCP	60 80 → 1585 [ACK] Seq=1 Ack=435 Win=2920 Len=0	
18 6.	257149	207.68.173.245	137.30.122.253	HTTP	666 HTTP/1.1 302 Found (text/html)	v
▷ Frame 1	3: 62 byte	es on wire (496 bits)), 62 bytes captured ((496 bits)		
Etherne	t II, Src	Apple_cc:57:92 (00:	:03:93:cc:57:92), Dst:	: CiscoInc_41:a8:44	0 (00:0d:ed:41:a8:40)	
Interne	t Protoco	l Version 4, Src: 137	7.30.122.253, Dst: 207	7.68.173.245		
Transmi:	ssion Cont	trol Protocol, Src Po	ort: 1585 (1585), Dst	Port: 80 (80), Sec	q: 0, Len: 0	
0000 00 0	0d ed 41 a	8 40 00 03 93 cc 57	92 08 00 45 00	A.@WE.		
0010 00	30 ca a7 4	40 00 80 06 ae ca 89) 1e 7a fd cf 44 .0.	@zD		
0020 ad 1	f5 06 31 0	00504dfd cd0a00	00 00 00 70 02	.1.PMp.		
0030 fa t	f0 e5 4f 0	00 00 02 04 05 b4 01	01 04 02	.0		
🔵 🍸 rhi	no				Packets: 6557 · Displayed: 6557 (100.0%) · Load time: 0	:0.515 Profile: Default

2. Identify clear text user name and password for FTP login

📕 rhind	log	pla l'alla				
<u>File</u>	dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>A</u> nalyze <u>S</u> tati	stics Telephony <u>W</u> ireless	<u>T</u> ools <u>H</u> elp		
	1 🔘] 🖪	े 🎗 🖒 🤇 🔶 🔿 🖻	₹↓,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Q. II		
Appl	/ a display filter	<ctrl-></ctrl->				Expression +
No.	Time	Source	Destination	Protocol	Length Info	
152	9 179.040214	137.30.120.40	137.30.122.253	FTP	82 Response: 220 cook FTP_server_ready.	
15	2 182.640647	137.30.122.253	137.30.120.40	FTP	66 Request: USER gnome	
153	4 182.644970	137.30.120.40	137.30.122.253	FTP	88 Response: 331 Password required for gnome.	
153	6 184.667754	137.30.122.253	137.30.120.40	FTP	69 Request: PASS gnome123	
153	8 184.748946	137.30.120.40	137.30.122.253	FTP	81 Response: 230 User gnome logged in.	
154	0 185.602553	137.30.122.253	137.30.120.40	FTP	62 Request: TYPE I	-
154	1 185.602818	137.30.120.40	137.30.122.253	FTP	74 Response: 200 Type set to I.	
154	4 188.994914	137.30.122.253	137.30.120.40	FTP	81 Request: PORT 137,30,122,253,6,121	
154	5 188.995519	137.30.120.40	137.30.122.253	FTP	84 Response: 200 PORT command successful.	
154	6 188.996081	137.30.122.253	137.30.120.40	FTP	71 Request: STOR rhino1.jpg	
155	0 189.033465	137.30.120.40	137.30.122.253	FTP	111 Response: 150 Opening BINARY mode data connection for rhino1.jp	g.
161	2 189.221711	137.30.120.40	137.30.122.253	FTP	78 Response: 226 Transfer complete.	
163	4 194.426879	137.30.122.253	137.30.120.40	FTP	60 Request: QUIT	
163	5 194.427484	137.30.120.40	137.30.122.253	FTP	104 Response: 221-You have transferred 65703 bytes in 1 files.	
163	6 194.432107	137.30.120.40	137.30.122.253	FTP	186 Response: 221-Total traffic for this session was 66042 bytes in	1 transfers.
162	3 195.462335	137.30.120.40	137.30.122.253	FTP	82 Response: 220 cook FTP server ready.	
162	5 198.525443	137.30.122.253	137.30.120.40	FTP	66 Request: USER gnome	
162	7 198.529854	137.30.120.40	137.30.122.253	FTP	88 Response: 331 Password required for gnome.	
▷ Fra	ne 1532: 66 b	ytes on wire (528 bits	;), 66 bytes captured	(528 bits)		
▷ Eth	ernet II, Src	: Apple_cc:57:92 (00:0	3:93:cc:57:92), Dst:	OracleCo_t0:13:96 (08:	00:20:10:13:96)	
▷ Int	ernet Protoco.	l Version 4, Src: 137.	30.122.253, Dst: 137.	30.120.40		
D Tra	ismission Con	trol Protocol, Src Por	rt: 1655 (1655), Dst P	ort: 21 (21), Seq: 1,	Ack: 29, Len: 12	
▷ Fil	e Transfer Pro	otocol (FTP)				
0000	08 00 20 f0 1	13 96 00 03 93 cc 57	92 08 00 45 00			
0010	00 34 d1 46 4	40 00 80 06 24 1b 89	1e 7a fd 89 1e .4.F	0\$z		
0020	78 28 06 77 0	00 15 50 db 34 c8 0d	d3 22 ea 50 18 x(.w	P. 4".P.		
0030	fa d4 05 89 0	00 00 55 53 45 52 20	67 6e 6f 6d 65	US ER gnome		
0040	0d 0a					
0 7	rhino				D-data SEE7 Displayed SEE7 (10)	0.0%) + Lord time: 0:0.515 Brofile: Defe
-	THE				Packets: 6557 * Displayed: 6557 (10)	, o ray - Load time, 0.0.315 Profile: Defau

3. Locate FTP-DATA protocol – the first file transferred by FTP-DATA protocol

	3. LO	cate FIP-D	ATA protoc	$o_1 - the first$	t file transferred by F I	P-DATA protocol	
🚄 rhino.	log				and the Research Street Annual Manha		
<u>F</u> ile <u>E</u> c	lit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> <u>Statis</u>	stics Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u> elp			
	1 💌 🌗 🛅) 🔀 🖸 । ९ 👄 👄 🕾	👔 🖢 🚍 🔲 🍳 Q	Q, 🎹			
Apply	a display filter ·	<ctrl-></ctrl->					Expression +
No.	Time	Source	Destination	Protocol	Length Info		*
564	5 485.713037	137.30.120.40	137.30.122.253	FTP	84 Response: 200 PORT command success	ful.	
564	7 485.713603	137.30.122.253	137.30.120.40	FTP	75 Request: STOR contraband.zip		
565	1 485.741255	137.30.120.40	137.30.122.253	FTP	115 Response: 150 Opening BINARY mode	data connection for contraband.zip.	
583	9 485.918543	137.30.120.40	137.30.122.253	FTP	78 Response: 226 Transfer complete.		
584	1 487.585054	137.30.122.253	137.30.120.40	FTP	60 Request: QUIT		
584	2 487.585467	137.30.120.40	137.30.122.253	FTP	105 Response: 221-You have transferred	230566 bytes in 1 files.	
584	8 487.589853	137.30.120.40	137.30.122.253	FTP	187 Response: 221-Total traffic for th	is session was 230914 bytes in 1 transfers.	
155	l 189.037516	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
155	2 189.037663	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
155	4 189.038191	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
155	5 189.038268	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
155	7 189.038368	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
155	3 189.038447	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
156	0 189.039167	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
156	1 189.039248	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
156	2 189.039328	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
156	4 189.040132	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		
156	5 189.040215	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 1460 bytes		v
<pre>▷ Fram ▷ Ethe ▷ Inte ▷ Tran FTP</pre>	e 1554: 1514 rnet II, Src rnet Protoco smission Cont Data (1460 by	bytes on wire (12112 : Apple_cc:57:92 (00:0 l Version 4, Src: 137. trol Protocol, Src Por ytes data)	bits), 1514 bytes capt 3:93:cc:57:92), Dst: 0 30.122.253, Dst: 137.3 t: 1657 (1657), Dst Po	ured (12112 bits) racleCo_f0:13:96 (08:0 0.120.40 rt: 20 (20), Seq: 2921	10:20:f0:13:96) ., Ack: 1, Len: 1460		
0000 0010 0020 0030 0040 0050 0060 0050 0060 0070 0080 0090	08 00 20 f0 1 05 dc d1 51 4 78 28 06 79 6 fa f0 0b 31 6 6a 37 9d bb 31 6 6a 37 9d bb 31 6 6d b7 9d 09 3 6 6d b5 9 9 b 5 9 5 bc b7 48 80 6 33 9 4 0e ae a cc 6b 0b 7d 1 1 1 1	13 96 00 03 93 cc 57 14 00 80 06 1e 68 89 14 01 80 06 1e 68 89 00 01 51 02 2e 80 04 00 00 0c cb fd 2b 40 00 00 0c cb fd 2b 40 00 00 bc cb fd 2b 40 04 05 bf fd 3b fd 40 05 05 fd fd 3b fd 7 9d 96 05 5b ff 4b 36 39 be 3d 95 53 1c 63 39 be 40 99 95 1c c6 35 1c 63 9c ib 16 ff	92 08 00 45 00 0g 1e 7a fd 99 1e 0g 1f 6a 56 0 x(.y. 0g 73 65 a3 73 0c 1 2a 39 98 ada j7 1a 96 6 f8				· · · · · · · · · · · · · · · · · · ·
0 🛛	rhino					Packets: 6557 · Displayed: 6557 (100.0%) · Load time: 0:0.	515 Profile: Default

4. Right click and choose follow TCP stream --- to recover a file transmitted by FTP-DATA

📕 ri	hino.log									
File	Edit	View Go	<u>Capture</u> <u>Analyze</u> <u>Sta</u>	atistics Telephony <u>W</u> irele	s <u>T</u> ools <u>H</u> elp					
4	I Ø	0 🔒 🗄	X 🖸 Q ⇔ ⇔ ⋸	2 T & 🗐 🗐 Q G	. 🔍 🎹					
$\overline{\Box}$	annly a c	display filter	<cħ-></cħ->							Expression +
	appiy u c	ларину плост			- · · · ·					
No.	1	lime	Source	Destination	Protocol	Length Info				F
	5646 4	485.713037	137.30.120.40	137.30.122.253	FTP	84 Response: 20	00 PORT command successfu	1.		L
	5647 4	485.713603	137.30.122.253	137.30.120.40	FTP	75 Request: STO	OR contraband.zip			
	5651 4	485.741255	137.30.120.40	137.30.122.253	FTP	115 Response: 15	50 Opening BINARY mode da	ta connection 1	for contraband.zip.	
	5839 4	485.918543	137.30.120.40	137.30.122.253	FTP	78 Response: 22	26 Transfer complete.			-
	5841 4	187.585054	137.30.122.253	137.30.120.40	FTP	60 Request: QUI				
	5842 4	187.585467	137.30.120.40	137.30.122.253	FIP	105 Response: 22	21-You have transferred 2	30566 bytes in	1 files.	
	5843 4	+87.589853	137.30.120.40	137.30.122.253	FIP DATA	187 Response: 22	21-lotal trattic for this	session was 2:	30914 bytes in 1 transfers	s.
	1551 1	189.037516	137.30.122.253	137.30.120.40	FTP-DATA	1514 FTP Data: 14	160 bytes			
-	1552 1	189.037663	137.30.122.255	137.30.120.40	FIP-DATA	1514 FIP Data: 14	100 bytes			
-	1554 1	180 038368	137.30.122.255	137.30.120.40		1514 FTP Data: 14	Mark/Upprack Dasket	Ciril M		
	1555 1	100 020200	127 20 122 252	127 20 120.40	FTP DATA	1514 FTP Data:	Mark/ Onmark Packet	CUITIN		
	100/ 1	109.030300	137.30.122.255	137.30.120.40	FTP-DATA	1514 FTP Data:	Ignore/Unignore Packet	Ctrl+D		
	1550 1	120 020167	127 20 122 252	127 20 120 40	FTP-DATA	1514 FTP Data:	Set/Unset Time Reference	Ctrl+T		
	1560 1	100 020249	137.30.122.233	127 20 120.40	ETR-DATA	1514 FTP Data:	Time Shift	Ctrl+Shift+T		
	1562 1	100 020220	137.30.122.233	137.30.120.40	ETD DATA	1514 FTP Data.		Control of the second		
	1562 1	120 040122	127 20 122 252	127 20 120.40	FTP-DATA	1514 FTP Data:	Packet Comment			
	1565 1	189.040132	137 30 122 253	137 30 120.40	ETR-DATA	1514 FTP Data.	Edit Recolved Name			
	1903 1	109.040215	157.50.122.255	157.50.120.40	TIF-DATA	1514 117 5868.	Edit Nesolved Name			
	rame	1554: 1514	bytes on wire (1211)	2 bits), 1514 bytes ca	otured (12112 bits)		Apply as Filter	•		
	Ethern	et II, Src	: Apple_cc:57:92 (00	:03:93:cc:57:92), Dst:	OracleCo_f0:13:96 (08:00:20:f0:13:96)	Prenare a Filter	•		
▷ :	Intern	et Protoco	l Version 4, Src: 13	7.30.122.253, Dst: 137	.30.120.40		riepore of files			
▷ .	fransm	ission Con	trol Protocol, Src Pe	ort: 1657 (1657), Dst	Port: 20 (20), Seq:	2921, Ack: 1, Len: 146	Conversation Filter	,		
	TP Da	ta (1460 b	ytes data)				Colorize Conversation	•		
							SCTP	•		
000	0 08	00 20 f0 1	13 96 00 03 93 cc 53	7 92 08 00 45 00	WE.		Follow	•	TCP Stream	
001	0 05	dc d1 51 4	40 00 80 06 le 68 89	9 1e 7a fd 89 1e	Q@hz				LIDB Stream	
002	0 78	28 06 79 0	00 14 51 02 2e d8 0d	d fb da 36 50 10 x(.	/Q6P.		Сору	•	obr Stream	
003	0 fa	+0 0b 31 0	00 00 b0 cb fd 2b 40	07365a3730c	1+@se.s.		Desta est Desferre est		SSL Stream	
004	0 6a	57 90 DD 9	90 09 0T ab 66 CT Ta 8 b1 ad ab dc 74 da	1 ez ao 99 da da j/. 1 1 a o 6 o 6 fa o 3	+		Protocol Preferences	, ,		
005	6 Cu	bb 59 e9 b	nd 35 h8 c7 79 ad 96	5 3h 23 12 81 h0 m.V			Decode <u>A</u> s			
007	0 bc	b7 48 80 0	5b 6f fa 4b 36 39 be	e ff 00 d1 2b faH	.ko.K 69+.		Show Packet in New Window	w		
008	0 39	b4 0e ae a	ad 99 95 31 cd 63 50	d 36 5b 60 d9 f9 9	1 .c]6[`	_	_			
009	0 cc	6b 0b 7d 1	fb ff 00 d2 7a bf 90	: 8f f5 77 07 a3 .k.	} zw					
•	7 d	hino						Packets: 6557 · Di	splayed: 6557 (100.0%) · Load time	: 0:0.515 Profile: Defau

5. The raw file recovered—file transferred by FTP-DATA Note the JFIF file signature from BYTE 6 to BYTE 9

Wireshark · Follow TCP Stream (tcp.stream eq 71) · rhino	<u> </u>	x
		_
		^
SBIM.		=
.88IM	obe	
Photoshop. 4.0Adobe.d		
······		
7GWgwCS.cs4.		
%&5D.TdEU6teuFk.2.p	iV	
1.0.#1. cf@0.Z.uh2.EM		
s.FQtv{.i.ZLH=~5.>8.>.i.%.c[.@H sr.2y.Eie^Z584.		
<pre></pre>	.L.Gc	
n.;.xCgV?5.}TN.A\$		
+8.R6ct.{.TF>E.		
.cMu;o.S[,c]?&F	Z.\.Y.a .?	
].~]@!d.8.).85.i,n.sGk[.R.bV0.]5g	BW.}.?	
D~!O.in.8.cs	edlqi.	
7{?		
q.&a>VR.'?.(T.\$o.].v.1.>.\;0ve.M[Sc7.s7.eW.sG1}07.	,ke.	
{		
E5]Bv@e.v;V.V.v.,?P.LE.QUZ22`coz?.o.W.=1p1.]L.uM&.}zj.w\.RM.		
({K&.cZ]2[^R"cl\$^R.Zj.kl.n.#M.		
/d.iKu;.j.jdXI~19.;;C;C;C;.J,Wvs	9.	
\@<		-
0 client oktás). 46 server oktás). 0 turns	F 461	-
Entire conversation (65 kB) Show data as ASCII	Stream 71	*
Find:	Find Next	
😰 💽 🥥 🥞 🥌 🏈 🔯	00-	

6. Save the file to a RAW format



8. Locate the file rhino.jpg and double click



HTTP Transmitted File Recovery

1. Open rhino2.log file in Wireshark and sort http protocol, and locate rhino4.jpg

	111102.109			_		
Eile	e <u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze	tatistics Telephony <u>W</u> ireles	s <u>T</u> ools <u>H</u> elp		
Â.	I 🖉 💿 🚺 🗄	े 🔀 🙆 🤇 😓 🔿	🛎 T 🞍 🗐 🗐 🔍 Q	0, 🎹		
	Apply a display filter	<ctrl-></ctrl->				Expression +
No.	Time	Source	Destination	Protocol	Lenath Info	
	4 0.089697	137.30.123.234	64,233,167,104	HTTP	356 GET / HTTP/1.1	
	11 0.774546	137, 30, 123, 234	64,233,167,104	HTTP	404 GET /images/logo.pif HTTP/1.1	
1	28 5,287376	137.30.123.234	137.30.120.37	HTTP	437 GET /~gpome HTTP/1.1	_
	30 5.301396	137.30.120.37	137.30.123.234	HTTP	642 HTTP/1.1 301 Moved Permanently (text/html)	
	32 5.554353	137.30.123.234	137.30.120.37	HTTP	438 GET /~gnome/ HTTP/1.1	
	34 5.638951	137.30.120.37	137.30.123.234	HTTP	1033 HTTP/1.1 200 OK (text/html)	
	36 5.900207	137.30.123.234	137.30.120.37	HTTP	325 GET /icons/blank.gif HTTP/1.1	
	37 5.905032	137.30.120.37	137.30.123.234	HTTP	484 HTTP/1.1 200 OK (GIF89a)	
4	39 6.160811	137.30.123.234	137.30.120.37	HTTP	326 GET /icons/image2.gif HTTP/1.1	
	43 6.163831	137.30.123.234	137.30.120.37	HTTP	324 GET /icons/back.gif HTTP/1.1	
11	45 6.166705	137.30.120.37	137.30.123.234	HTTP	646 HTTP/1.1 200 OK (GIF89a)	
	46 6.171826	137.30.120.37	137.30.123.234	HTTP	553 HTTP/1.1 200 OK (GIF89a)	
T.	49 7.892558	137.30.123.234	137.30.120.37	HTTP	488 GET /~gnome/rhino4.jpg HTTP/1.1	
+	215 8.094061	137.30.120.37	137.30.123.234	HTTP	273 HTTP/1.1 200 OK (JPEG JFIF image)	
	217 14.008741	137.30.123.234	137.30.120.37	HTTP	488 GET /~gnome/rhino5.gif HTTP/1.1	
	312 14.197534	137.30.120.37	137.30.123.234	HTTP	675 HTTP/1.1 200 OK (GIF89a)	
	333 27.886521	137.30.123.234	64.233.167.104	HTTP	356 GET / HTTP/1.1	
	343 43.918664	137.30.123.234	137.30.120.37	HTTP	439 GET /~venkata HTTP/1.1	-
⊳	Frame 49: 488 by	tes on wire (3904 b	its), 488 bytes capture	(3904 bits)		
\triangleright	Ethernet II, Src	: Apple_cc:57:92 (0	0:03:93:cc:57:92), Dst:	OracleCo_72:6	if:0b (08:00:20:72:6f:0b)	
⊳	Internet Protoco	l Version 4, Src: 1	37.30.123.234, Dst: 137	30.120.37		
⊳	Transmission Con	trol Protocol, Src	Port: 2026 (2026), Dst H	ort: 80 (80),	Seq: 1311, Ack: 2590, Len: 434	
⊳	Hypertext Transf	er Protocol				
00	00 08 00 20 72	6f 0b 00 03 93 cc	57 92 08 00 45 00	юWЕ.		*
00	10 01 da ab 89 4	40 00 80 06 47 48	89 1e 7b ea 89 1e	@ GH{		
00	20 78 25 07 ea	00 50 5b 35 13 ec	49 29 bb 11 50 18 x%.	.P[5I)P.		E
00	30 f6 f2 08 19 0	00 00 47 45 54 20	2f 7e 67 6e 6f 6d	GE T /~gnom	1	
00	40 65 2f 72 68	69 6e 6f 34 2e 6a	70 67 20 48 54 54 e/r	ino4 .jpg HTT		
00	50 50 2f 31 2e	31 0d 0a 41 63 63	65 70 74 3a 20 69 P/1	1A ccept: i		
00	00 60 61 67 65 3	21 07 69 66 2C 20	09 00 01 0/ 05 2T mage	/git , image/		
00	80 2f 6a 70 65	67 2c 20 69 6d 61	67 65 2f 70 6a 70 /in	g, i mage/pir		
00	90 65 67 2c 20	61 70 70 6c 69 63	61 74 69 6f 6e 2f eg,	appl ication/		
	7 chine?		0,		Deductor 270 (Displayed, 270 (100 00() + 11 4 0.0 0	Profiles Defende
0	- minoz				Packets: 570 * Displayee: 570 (100.0%) * Load time: 0:0.0	Profile: Default
	\mathbf{T}	11 TOI			41 . 61	

2. Follow TCP stream to recover this file

	rhino2.log					
F	ile Edit View Go	Capture Analyze	Statistics Telephony Wireles	s Tools Help		
4	(🔳 🖉 💿 🌗 🖡	े 🗙 🖾 🔍 🔶 🔿	🕾 T 🖢 🗔 🗐 Q, Q	. 🔍 🎹		
Γ.	Apply a display filter	<ctrl-></ctrl->				Expression +
N	, Time	Source	Destination	Protocol	Length Info	A
	4 0.089697	137.30.123.234	64,233,167,104	HTTP	356 GET / HTTP/1.1	
	11 0,774546	137.30.123.234	64,233,167,104	HTTP	404 GET /images/logo.gif HTTP/1.1	_
	28 5.287376	137.30.123.234	137.30.120.37	нттр	437 GET /~gnome HTTP/1.1	
	30 5.301396	137.30.120.37	137.30.123.234	HTTP	642 HTTP/1.1 301 Moved Permanently (text/html)	
	32 5.554353	137.30.123.234	137.30.120.37	HTTP	438 GET /~gnome/ HTTP/1.1	
	34 5.638951	137.30.120.37	137.30.123.234	HTTP	1033 HTTP/1.1 200 OK (text/html)	
	36 5.900207	137.30.123.234	137.30.120.37	HTTP	325 GET /icons/blank.gif HTTP/1.1	
	37 5.905032	137.30.120.37	137.30.123.234	HTTP	484 HTTP/1.1 200 OK (GIF89a)	
+	39 6.160811	137.30.123.234	137.30.120.37	HTTP	326 GET /icons/image2.gif HTTP/1.1	
	43 6.163831	137.30.123.234	137.30.120.37	HTTP	324 GET /icons/back.gif HTTP/1.1	
	45 6.166705	137.30.120.37	137.30.123.234	HTTP	646 HTTP/1.1 200 OK (GIF89a)	
	46 6.171826	137.30.120.37	137.30.123.234	HTTP	553 HTTP/1.1 200 OK (GIF89a)	
4	49 7.892558	137.30.123.234	137.30.120.37	HTTP	488 GET /~gnome/rhino4.ipg HTTP/1.1	
1 +	215 8.094061	137.30.120.37	137.30.123.234	HTTP	Mark/Unmark Packet Ctrl+M	
	217 14.008741	137.30.123.234	137.30.120.37	HTTP	4 Ignore/Unignore Packet Ctrl+D	
	312 14.197534	137.30.120.37	137.30.123.234	HTTP	6 Set/Uncet Time Reference Ctrle T	-
	333 27.886521	137.30.123.234	64.233.167.104	нттр	Set of set of the reference of the set	
	343 43.918664	137.30.123.234	137.30.120.37	нттр	Ime Shift Ctrl+Shift+1	· ·
Þ	Frame 49: 488 by	tes on wire (3904 b	oits), 488 bytes capture	d (3904 bits)	Packet Comment	
Þ	Ethernet II, Sro	: Apple cc:57:92 (0	0:03:93:cc:57:92), Dst:	OracleCo 72:6f:0b (08:	8:00:20	
Þ	Internet Protoco	1 Version 4, Src: 1	137.30.123.234, Dst: 137	.30.120.37	Edit Kesolved Name	
Þ	Transmission Con	trol Protocol, Src	Port: 2026 (2026), Dst H	Port: 80 (80), Seq: 131	311, Ack Apply as Filter	
Þ	Hypertext Transf	er Protocol				
					Prepare a Hitter	
					Conversation Filter	
0	000 08 00 20 72	6f 0b 00 03 93 cc	57 92 08 00 45 00	roWE.	Colorize Conversation +	<u>^</u>
0	010 01 da ab 89	40 00 80 05 47 48 00 50 55 35 13 ec	89 1e /D ea 89 1e	.@ GH{ p[s t) p	SCTP +	=
0	030 f6 f2 08 19	00 00 47 45 54 20	2f 7e 67 6e 6f 6d	GE T /~gnom		
0	040 65 2f 72 68	69 6e 6f 34 2e 6a	70 67 20 48 54 54 e/rl	nino4 .jpg HTT	ronow rCP Stream	
0	050 50 2f 31 2e	31 0d 0a 41 63 63	65 70 74 3a 20 69 P/1	.1A ccept: i	Copy UDP Stream	
0	060 6d 61 67 65	2f 67 69 66 2c 20	69 6d 61 67 65 2f mag	e/gif , image/	SSL Stream	
0	070 78 2d 78 62	69 /4 60 61 70 2c	20 69 60 61 67 65 x-x	oitma p, image	Protocol Preferences +	
0	090 65 67 2c 20	61 70 70 6c 69 63	61 74 69 6f 6e 2f eg.	appl ication/	Decode As	
Ľ					Show Packet in New Window	-
(🥑 🛃 rhino2				Packets: 370 · Displayed: 370 (100.0%) · Load time: 0:0.0	Profile: Default

3. Save the file as raw to rhino4.jpg, compare the raw format and ASCII format (http? Not JFIF from byte 6 at the beginning)



Wireshark - Follow TCP Stream (tcp.stream eq 1) - rhino2	
GET /~gnome HTTP/1.1 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms- application/msword, application/x-shockwave-flash, */*	-powerpoint,
Accept-Language: en-us 	
Host: www.cs.uno.edu Connection: Keep-Alive	
HTTP/1.1 301 Moved Permanently Date: Wed, 28 Apr 2004 21:07:25 GMT Server: Apache/1.3.29 (Unix)	
Location: http://www.cs.uno.edu/~gnome/ Keep-Alive: timeout=15, max=100 Connection: Keep-Alive	
Transfer-Encoding: chunked Content-Type: text/html; charset=iso-8859-1	
130 HTML PUBLIC "-//IETF//DTD HTML 2.0//EN" <html><head></head></html>	
<title>301 Moved Permanently</title> <body> <h1>Moved Permanently</h1></body>	
The document has moved here . <p> <hr/> <address>Apache/1.3.29 Server at www.cs.uno.edu Port 80</address></p>	
<pre>GET /~gnome/ HTTP/1.1 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms- application/msword, application/x-shockwave-flash, */* Accept-Language: en-us</pre>	-powerpoint,
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322) Host: www.cs.uno.edu	
Packet 30. 5 client pkt(s), 112 server pkt(s), 9 turns. Click to select. Entire conversation (157 kB) Show data as	Stream 1 💭
Find:	Find <u>N</u> ext
8 0 4 🚔 🔌 🏈 💵 📶	- m.) [.m.)



5. Open the file in a hex editor, xvi32

32 - rhino4.jpg	(m. # . # .)	
idit Search Address Bookmarks Tools XVIscript Help		
Paul A & House, Grand Strates	47 45 54 20 2F 78 67 68 6F 6D 65 20 48 54 50 2F 31 2F 31 00 03 41 63 63 65 70 74 33 20 65 6D 61 67 69	5 22 57 59 55 20 20 *
29 image/x-xbitmap, image/jpeg, image/pjpe	g , 65 6D 61 67 65 27 76 20 78 60 74 6D 61 70 20 20 69 6D 61 67 65 27 6A 70 65 67 20 20 69 6D 61 67 65 27 70 20 70 60 70 70 70 70 70 70 70 70 70 70 70 70 70	F 70 6A 70 65 67 2C
52 application / vnd.ms = excel, application /	v n 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 6C 2C 20 61 70 70 6C 69 63 61 74	4 69 6F 6E 2F 76 6E
75 d.ms-powerpoint, application/msword, ap	p 1 64 22 6D 73 2D 70 67 77 65 72 70 67 67 65 72 70 67 63 74 2C 20 61 70 70 6C 65 63 61 74 65 67 62 27 6D 73 77 67 72 6	4 2C 20 61 70 70 6C
As ication/x-shockwave-flash, */* Accept-	L a 69 63 61 74 69 67 62 27 78 20 73 65 67 63 68 77 61 76 65 20 66 6C 61 73 68 22 20 24 27 24 00 04 61 63 63	3 65 70 74 2D 4C 61 D 2D 2D 20 2D 2D 2D 2D
re User-Agent: Mozilla/4.0 (compatib	1 e 3D 2D 2D 2D 0D 0A 55 73 65 72 2D 41 67 65 62 74 3A 20 4D 67 7A 69 6C 6C 61 27 34 22 30 20 28 63 67 6D 70	0 61 74 69 62 60 65
11F / M8IE 6.0/ Windows NT 6.1/ .NET CLR 1.	1 _ 38 20 40 53 49 45 20 36 22 30 38 20 57 69 62 64 6F 77 73 20 42 54 20 35 22 31 38 20 22 42 45 45 20 43 40	C 52 20 31 28 31 28
149 4322) Rost: www.cs.unc.edu Connection	24 33 32 32 32 39 0D 0A 48 6F 73 74 3A 30 77 77 77 22 63 73 3E 75 6E 6F 22 65 64 75 0D 0A 43 6F 6E 6E 6E 6E 6E 6	3 74 69 6F 6E 3A 20
15A bly Date: Wed, 28 Apr 2004 21:07:28 GM	T 74 6C 79 0D 0A 44 61 74 65 3A 20 57 65 64 2C 20 32 38 20 41 70 72 20 32 30 34 20 32 31 3A 30 37 3A 33	Z 35 20 47 4D 54 0D
1C3 8 e x v e x : A p a e h e / 1 . 8 . 2 9 (U n i x) L o e a t i o n	1 0A 53 65 72 76 65 72 3A 20 41 70 61 63 69 65 2F 31 2E 33 2E 32 39 20 28 55 6E 69 78 29 0D 0A 4C 6F 63 65	1 74 69 6F 6E 3A 20
<pre>EC http://www.cs.uno.edu/-gnome/ Keep-Ali</pre>	v = 60 74 74 70 3A 2F 2F 77 77 72 2E 63 73 2E 75 6E 6F 2E 65 64 75 2F 7E 67 6E 6F 65 65 2F 0D 0A 4B 65 65 70	0 2D 41 6C 69 76 65
38 live Transfer-Encoding: chunked Conse		3 6F 6E 74 65 6E 74
67 - Type: text/html; charset=iso-9959-1	1 25 54 79 70 65 28 20 74 65 78 74 27 68 74 65 66 28 20 62 68 61 72 73 65 74 25 69 72 67 20 28 28 25 29 20	D 21 0D 0A 0D 0A 21
90 3 0 4 1 D 0 C T Y P E H T H L P U B L I C " - / / I E T F / / D T D	II 33 30 0D 0A 3C 21 44 4F 43 54 59 50 45 20 40 54 4D 4C 20 50 55 54 24 C 49 43 20 22 2D 2F 2F 49 45 54 46 22	T 2T 44 54 44 20 40
2 ed Permanently 7111LE <80DY> <#	1 > 65 420 50 65 72 60 61 62 66 72 46 62 73 62 79 54 49 54 42 45 32 0A 32 27 54 84 54 14 43 22 42 44 54	9 3E 0A 3C 48 31 3E
Moved Permanently The document has	m 4D 6F 76 65 64 20 50 65 72 6D 61 6E 65 6E 74 6C 79 3C 2F 48 31 3E 0A 54 68 65 20 64 6F 63 75 6D 65 6E 74	4 20 60 61 73 20 6D
4 oved < A HREF="http://www.cs.uno.edu/~gn	o m 67 76 65 64 20 3C 41 20 48 52 45 46 3D 22 68 74 74 70 3A 27 27 77 77 77 22 63 73 22 75 62 67 24 24 56 64 75	5 2F 7E 67 6E 6F 6D
6 .29 Server at www.cs.uno.edu Port 80 <td></td> <td>0 00 00 27 01 28 00 0 20 2C 27 41 44 44</td>		0 00 00 27 01 28 00 0 20 2C 27 41 44 44
J R E S S > < / B O D Y > < / H T M L > 0 G E T / ~ g n o m e	/ 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C 2F 48 44 59 A 3C 2F 48 54 4D 4C 3E 0A 0D 0A 30 0D 0A 0D 0A 47 45 54 20 2F 7E 6	7 6E 6F 6D 65 2F 20
/8 H T T P / 1 . 1 A c c e p 5 : i m a g e / g i f , i m a g e / x - x b	1 b 6 5 6 5 6 5 7 6 5 6 5 2 7 3 1 2 5 3 1 0 D 0 A 4 1 6 3 6 3 6 5 7 0 7 4 3 A 2 0 6 5 6 D 6 1 6 7 6 5 2 7 6 7 6 5 6 5 2 2 0 6 5 6 D 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 7 6 5 2 7 6 7 6 5 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6 1 6 1	F 78 2D 78 62 69 74
A /vnd.ms=excel, application/vnd.ms=power		0 GF 77 G5 72 70 GF
3 int, application/msword, application/x-	n h 69 62 74 2C 20 61 70 70 6C 69 63 61 74 69 67 62 27 6D 73 77 67 72 64 2C 20 61 70 70 6C 69 63 61 74 69 65	r 6E 2F 78 2D 73 68
Cockvave-flash, */* Accept-Language: en	- u 67 63 68 77 61 76 65 2D 66 6C 61 73 68 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 74 2D 4C 61 68 67 75 61 67 66	5 3A 20 65 6E 2D 75
Z gent: Mozilla/4.0 (compatible/ MSIE 6.0	A 73 DD 0A 2D	5 20 36 22 30 35 20
7 Windows NT 6.1 NET CLR 1.1.4322) Hos	5 : 57 59 58 54 57 77 73 20 42 54 20 35 22 31 38 20 28 42 55 40 20 43 40 52 20 31 22 31 28 34 33 32 32 32 50	D 0A 48 6F 73 74 3A
0 vvv.os.uno.edu Conneotion: Keep-Alive		1 6C 69 76 65 0D 0A
0 Char dec: 71 Overwrite		
6 Search IEIE by using	wi search tab, you locate the IEIE file	gionatura
0. Scarch If If Uy using	AVI Scarch (ab, you locale the JTTT The	Signature
2 - rhino4 ing		
2 million, jpg		
dit Search Address Bookmarks Lools XVIscript Help		
IXIBBQ of B & M		
20 1 1 ve Content Type: image/jpeg	9 Ø 9 à + 1 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 69 6D 61 67 65 2F 6A	70 65 67 0D 0A 0D 0A FF D8 FF E0 00 1
FO 1 tree Content-Type: image/jpeg 19 EIF , , yp + U-Lead Systems, I	9 0 9 4 1 1 6 65 65 76 65 00 0A 43 65 65 74 65 65 74 20 54 79 70 65 3A 20 65 6D 61 67 65 27 6A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	70 65 67 0D 0A 0D 0A FF D8 FF E0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 FF D
Itema Content-Type: image/jpeg 19 217 , , yp 10 Lead Systems, I 24 B-2:2 2: B:6:05 6: 6: 5:	9 0 9 4 4 1 60 5 76 6 5 00 0 4 43 67 62 74 65 62 74 20 54 79 70 65 33 20 69 60 61 67 65 22 63 n c . 9 0 46 49 46 00 01 00 01 01 20 01 20 01 20 00 07 FF 25 00 17 55 20 40 65 61 64 20 53 79 73 4 4 9 9 9 9 9 64 00 42 20 23 33 22 9 42 33 56 33 48 47 42 47 64 37 60 45 65 66 60 52 53 79 73	70 65 67 0D 0A 0D 0A FF D8 FF E0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 FF D A7 F2 D5 FE FA EE D5 EA E5 FF FF FF FF
Item Content-Type: image/jpeg 19 Izz , , , , , , , , , , , , , , , , , , ,	9 9 9 4 4 4 6 65 10 0.4 13 12 14 15 15 10 15 12 14 15 15 15 15 15 15 15 15 15 15 15 15 15 16	70 65 67 0D 0A 0D 0A FF D8 FF E0 00 1 74 65 67 32 C2 04 96 63 22 00 FF A7 F2 D5 FE FA EE D5 EA 55 FF FF FF F A8 85 64 57 64 C4 65 65 C6 C6 FF FF FA
1 1	9 9 9 4 4 6 6 0 0 4 6 7 4 6 7 6 5 0 0 4 6 7 4 6 7 6 6 0 0 1 0 1 7 0 5 3 2 6 6 6 0 1 0 1 0 1 0 1	70 65 67 00 0A 0D 0A FF D8 FF E0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 FF D A7 F2 D5 FE FA EE D5 EA E5 FF FF FF 48 48 64 57 64 C4 6C C6 C4 FF FF EA F
1 Content - Type: Image/jpeq 1 XX , , , , , , , , , , , , , , , , , , ,	9 9 9 4 4 9 9 9 4 4 6 6 10 0 10 12 0 12 12 12 10 15 50 16 6 16 <t< td=""><td>70 65 67 0D 0A 0D 0A FF De FF E0 0 1 74 65 60 73 2C 20 49 6E 63 2E 0F FD A7 72 05 FE FA EE 05 EA E5 FF FF F F FF FF</td></t<>	70 65 67 0D 0A 0D 0A FF De FF E0 0 1 74 65 60 73 2C 20 49 6E 63 2E 0F FD A7 72 05 FE FA EE 05 EA E5 FF FF F F FF
1 1	$ \begin{array}{c} g \circ g \circ 4 & 4 \\ n \circ - & g \circ 0 \\ n \circ - & g \circ 0 \\ 1 & g \circ 0 \\ 2 & g \circ 0 \\ 1 & g \circ 0 \\ 2 & g \circ 0 \\ 1 & g \circ 0 $	70 65 67 00 0A 0D 0A FF DB FF DB 0 0 17 74 65 61 73 2 20 49 65 63 22 0 FF DA FF DA FF DA FF DA FF DA FF
1 1 Content - Type: 1 1 1 13 5 1 ,	y y y 4 + </td <td>70 65 67 0D 0A 0D 0A FF DE 0F 0 0 17 74 65 6D 73 2C 20 49 6E 63 2C 00 FF D 0A FF DE 0A DE 0A DE DE A FF DE DE FF DE DE</td>	70 65 67 0D 0A 0D 0A FF DE 0F 0 0 17 74 65 6D 73 2C 20 49 6E 63 2C 00 FF D 0A FF DE 0A DE 0A DE DE A FF DE DE FF DE
1 1	$ \begin{array}{c} 9 & 9 & 4 \\ 1 & 4 \\ 1 & 0 \\ 2 & 9 \\ 2 & 9 \\ 1 & 1 \\ 2 & 1 \\ 3 & 1 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 4 & 1 \\ 3 & 1 \\ 4 & 1 \\ 4 & 1 \\ 3 & 1 \\ 4 $	70 65 67 00 0A 0D 0A FT B8 FT E0 00 1 74 65 60 73 20 20 49 6E 63 2E 00 FT D A7 F2 06 FE FA E0 5E A5 FT FF FF 84 86 64 73 64 C4 6C 6C C4 FT FT E7 85 FT 65 FT 64 C4 6C 6C C4 FT FT E7 90 00 00 02 02 03 04 55 06 07 06 95 0 0A 08 10 00 02 01 03 03 02 40 03 05 0A 08 10 03 24 20 13 55 20 14 03 35
0 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 1	y y y 4 + </td <td>70 66 67 00 0A 0D 0A FF DB FF E0 00 1 74 66 67 0D 0A 0D 0A FF DB FF E0 00 1 74 75 0E FF FA ED 65 A 55 FF FF FF F 75 FF FF 75 FF FF FF FF FF FF FF FF FF FF 70 00 00 00 10 00 0A 04 05 65 77 85 FF FF FF 80 00 10 00 10 00 0A 04 05 60 70 80 90 AL 08 20 42 84 CL 15 52 0L F0 40 80 0</td>	70 66 67 00 0A 0D 0A FF DB FF E0 00 1 74 66 67 0D 0A 0D 0A FF DB FF E0 00 1 74 75 0E FF FA ED 65 A 55 FF FF FF F 75 FF FF 75 FF FF FF FF FF FF FF FF FF FF 70 00 00 00 10 00 0A 04 05 65 77 85 FF FF FF 80 00 10 00 10 00 0A 04 05 60 70 80 90 AL 08 20 42 84 CL 15 52 0L F0 40 80 0
1 1	$ \begin{array}{c} y \circ y \circ 4 & 4 & 4 \\ z \circ 5 & z \circ 76 & 65 & 00 & 0.4 & 0.5 & cs & cs & cs & 74 & 25 & 65 & 77 & 0.6 & 50.4 & 20 & 69 & 60 & 61 & 67 & 65 & 27 & 64.5 \\ z \circ 5 & z \circ 5 & z \circ 5 & z \circ 5 & 00 & 0.5 & 0.0 & 20 & 0.2 & 0.0 &$	70 66 67 00 0A 0D 0A FF D8 FF E0 00 1 74 66 60 70 2C 2D 95 66 2Z 50 FF D 74 65 60 70 2C 2D 95 66 2Z 50 FF D 74 65 60 70 2C 2D 95 66 2Z 50 FF D 75 FF FF 2F FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF FF 75 FF FF 75 FF
1 1 Content 1 y y 1 y </td <td>y 0 y 4 + 4 0 6 6 0 0 4 6 7 4 5 8 7 10 5 30 6 6 6 0 0 10 12 0 0 7 10 5 30 0 6 6 10 0 10 12 0 10 17 55 20 45 6 6 10 0 10 12 0 10 17 55 20 45 6 6 10 0 10 12 10 12 10 17 15 20 45 16 41 10 <</td> <td>70 65 67 00 0A 0D 0A FT 0B FF 0A 0C 0A FT 0C 0C 0C FT FT<</td>	y 0 y 4 + 4 0 6 6 0 0 4 6 7 4 5 8 7 10 5 30 6 6 6 0 0 10 12 0 0 7 10 5 30 0 6 6 10 0 10 12 0 10 17 55 20 45 6 6 10 0 10 12 0 10 17 55 20 45 6 6 10 0 10 12 10 12 10 17 15 20 45 16 41 10 <	70 65 67 00 0A 0D 0A FT 0B FF 0A 0C 0A FT 0C 0C 0C FT FT<
1 1	$ \begin{array}{c} y \circ y \circ 4 & 4 & 4 \\ z \circ y \circ y \circ 4 & 4 & 5 \\ z \circ y \circ y \circ y & 5 \\ z \circ y \circ y \circ y & 5 \\ z \circ y \circ y \circ y & 5 \\ z \circ y \circ y \circ y & 5 \\ z \circ z$	70 66 67 00 0A 0D 0A FF D8 FF E0 00 1 74 66 60 70 2C 2D 95 66 2Z 50 FF D 74 56 60 70 2C 2D 95 66 2Z 50 FF D 75 76 26 65 74 2C 2D 95 66 2Z 50 FF D 75 77 75 75 75 75 77 75 77 75 77 75 77 75 75 75 75 77 75 77 75 77 75 77 75 75 75 75 77 75 77 75 75 76 90 00 00 02 02 03 03 05 06 70 06 05 0 00 00 00 02 02 03 03 05 05 07 06 05 0 10 65 25 64 25 56 57 18 55 55 55 66 66 95 95 A2 A3 A4 A5 66 A7 A8 A3 A3 A5 85 56 25 76 25 A5 75 75 75 75 75 75 75
1 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 0	y 0 y 4 + C C D A S C C C D C C D A S C C C D C C D A S C C C D C C D C C D C C D C C D C C D C C D C C D C D C D C D C D C D C D C D C D C D C D C D C D <thd< th=""> D D D</thd<>	70 65 67 00 0A 0D 0A FF D8 FF D0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 7T D 74 75 0E 7F FA ED 5A 6E 65 7F FF FF 7 7F 7D 6E 7F FA ED 5A 6E 65 7F FF FF 7 7F 7F 7
1 1	9 9 9 4 4 6 6 0 0 0 1 1 1 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
1 1 0 1 1 0 1 1 0 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0	y y y 4 + </td <td>70 66 67 00 0A 0D 0A FF D8 FF D0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 FT D 74 75 0E FF FA ED 65 A 55 FF FF FF 7 75 75 0A 64 57 64 CC CC C4 FF FF FA 7 75 75 FF FF 75 75 FF FF FF FF FF 7 76 0A 0B 10 00 20 10 30 30 20 40 80 50 A1 08 24 53 46 56 56 55 55 55 65 64 64 99 3A 22 A3 A4 A5 A6 A7 A8 A3 A8 D2 1 84 65 FE FF FF 75 75 75 75 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 85 75 75 75 75 75 75 75 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 85 75 75 75 75 75 75 75 75 75 75 75 75 85 75 75 75 75 75 75 75 75 75 75 75 75 75</td>	70 66 67 00 0A 0D 0A FF D8 FF D0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 FT D 74 75 0E FF FA ED 65 A 55 FF FF FF 7 75 75 0A 64 57 64 CC CC C4 FF FF FA 7 75 75 FF FF 75 75 FF FF FF FF FF 7 76 0A 0B 10 00 20 10 30 30 20 40 80 50 A1 08 24 53 46 56 56 55 55 55 65 64 64 99 3A 22 A3 A4 A5 A6 A7 A8 A3 A8 D2 1 84 65 FE FF FF 75 75 75 75 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 84 65 75 12 85 A7 74 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 85 75 75 75 75 75 75 75 75 75 75 75 75 84 65 75 12 85 2A 71 75 75 75 75 75 85 75 75 75 75 75 75 75 75 75 75 75 75 85 75 75 75 75 75 75 75 75 75 75 75 75 75
1 1	9 9 9 9 9 9 9 9 9 9 9 9 1 1 1 6 6 9 6 9 7 6 9 9 9 6 6 9 0 1 6 9 0 1 6 9 0 1 6 9 1	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
1 1	y y	70 65 67 00 0A 0D 0A FT 0B FT 0A 0C 0A FT 0A 0A 0C 0C 0A 0T 0A 0A<
1 1	9 9	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	y 0 y 4 + <td>70 66 67 00 0A 0D 0A FT D8 FF E0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 FT D 74 75 0E FE FA E0 6 FA 65 FF FF FF F 75 FF FF FF FF FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF FF 76 00 00 10 20 20 10 80 30 20 40 80 50 A1 08 24 84 64 65 46 57 86 59 86 70 80 80 A1 08 24 84 84 84 65 66 75 85 55 86 86 66 99 9A 22 A3 A4 A5 A6 A7 A8 A9 AA 22 91 30 42 54 54 65 78 85 95 84 A2 23 24 84 55 66 77 85 95 84 A2 23 24 24 92 42 34 24 34 C1 15 52 00 17 04 80 50 11 06 12 40 20 10 80 30 20 40 80 50 11 06 12 40 20 10 80 30 20 40 80 50 11 06 12 43 54 65 66 77 85 95 86 86 64 64 99 9A 22 A3 A4 A5 A6 A7 A8 A9 A8 A2 B 84 55 86 77 85 95 84 A2 32 32 42 72 82 92 A3 85 86 87 88 93 A3 43 44 4 73 82 83 85 86 87 88 98 A3 93 A2 44 74 82 84 85 86 87 88 98 A3 93 A2 44 74 82 84 85 86 87 88 98 A4 20 70 80 90 70 70 76 70 76 00 20 12 10 10 91 70 10 10 FT 70 A0 80 90 90 91 10 10 10 10 10 10 10 70 70 A0 80 90 90 91 10 10 10 10 10 10 70 A0 80 90 91 91 90 90 12 10 10 91 91 10 10 FT 70 A0 80 91 91 90 90 91 10 10 10 10 10 70 70 A0 80 91 91 90 90 80 40 40 40 70 70 70 70 70 70 70 70 70 70 70 70 70</td>	70 66 67 00 0A 0D 0A FT D8 FF E0 00 1 74 65 6D 73 2C 20 49 6E 63 2E 00 FT D 74 75 0E FE FA E0 6 FA 65 FF FF FF F 75 FF FF FF FF FF FF FF FF FF FF 75 FF FF FF FF FF FF FF FF FF FF 76 00 00 10 20 20 10 80 30 20 40 80 50 A1 08 24 84 64 65 46 57 86 59 86 70 80 80 A1 08 24 84 84 84 65 66 75 85 55 86 86 66 99 9A 22 A3 A4 A5 A6 A7 A8 A9 AA 22 91 30 42 54 54 65 78 85 95 84 A2 23 24 84 55 66 77 85 95 84 A2 23 24 24 92 42 34 24 34 C1 15 52 00 17 04 80 50 11 06 12 40 20 10 80 30 20 40 80 50 11 06 12 40 20 10 80 30 20 40 80 50 11 06 12 43 54 65 66 77 85 95 86 86 64 64 99 9A 22 A3 A4 A5 A6 A7 A8 A9 A8 A2 B 84 55 86 77 85 95 84 A2 32 32 42 72 82 92 A3 85 86 87 88 93 A3 43 44 4 73 82 83 85 86 87 88 98 A3 93 A2 44 74 82 84 85 86 87 88 98 A3 93 A2 44 74 82 84 85 86 87 88 98 A4 20 70 80 90 70 70 76 70 76 00 20 12 10 10 91 70 10 10 FT 70 A0 80 90 90 91 10 10 10 10 10 10 10 70 70 A0 80 90 90 91 10 10 10 10 10 10 70 A0 80 90 91 91 90 90 12 10 10 91 91 10 10 FT 70 A0 80 91 91 90 90 91 10 10 10 10 10 70 70 A0 80 91 91 90 90 80 40 40 40 70 70 70 70 70 70 70 70 70 70 70 70 70
1 1	9 9 9 1 1 6 6 7 6 6 6 7 6 7 6 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 9 4 4 6 6 7 6 5 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
1 1	y y	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 9 4 4 6 6 7 6 6 7 6 6 7 6 7 6 7 6 7 6 7 6 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
1 1	y y	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 9 4 4 6 6 7 6 6 7 6 6 7 6 6 7 6 7 6 7 6 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
1 1 <th1< th=""> <th1< th=""> <th1< th=""> <th1< th=""></th1<></th1<></th1<></th1<>	9 9 9 1 1 6C 65 76 65 00 10 13 62 65 76 65 00 10	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 9 4 4 6 6 7 6 5 7 6 5 7 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	y y	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 9 4 4 6 6 7 6 5 7 6 5 7 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
1 1 0 1 <th1< th=""> 1 <th1< th=""> <th1< th=""></th1<></th1<></th1<>	y y	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 9 4 4 6 6 7 6 5 7 6 5 7 7 5 7 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
1 1	y y	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 4 4 6 6 7 6 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	y y	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
N N	9 9 4 4 6 6 7 6 6 7 6 6 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 4 4 6 6 7 6 6 7 6 6 7 6 7 6 7 6 6 7 6 7 6 6 7 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	9 9 4 4 6 6 7 6 6 7 6 6 7 6 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
N N	9 9 1 1 6C 69 76 60 10	$\begin{array}{cccccccccccccccccccccccccccccccccccc$

Adv. dec 4.522 7. Cut the http header, by using xvi/edit/delete to cursor (the last menu option)

XVI32 - rhin	no4.jpg		x
File Edit Se	earch Address Bookmarks	ools XVIscript Help	
D Ins	ert string	k?	
Ov	erwrite string	, y J U - Leiad Systems, I 77 DeFFE000010434649460001001012C012C0000FFF20017552D4C6561642053797374656D732C20	49 🔺
		6 : K G B O d S 1 d [[d Î ' š y S ò Õ þúí Č 62 63 22 00 FF DB 00 84 00 42 2D 32 3A 32 29 42 3A 36 3A 4B 47 42 4F 64 A7 6C 64 5B 5B 64 CC 92 9A 79 A7 F2 D5 FE FA EE	DS -
BIO	CK Mark Ctri+B	99999999999999999999999999999999999999	6C
Blo	ick <n> chars</n>	y y y y y y y y y y y y y y y y y y y	FF
Blo	ck unmark Ctrl+U	e	04
Pla	ck dalata Ctd. D	1 L J C 3 + 1 L 05 06 07 08 09 0A 0B 01 00 03 01 01 01 01 01 01 01 01 00 00 00 00 00	03
DIO	City City	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	15
BIO	Ctri+K	• () • 4 5 6 7 8 9 : C D E F G H I J S T U V W 52 D I F0 24 33 62 72 82 09 0A 16 17 18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A 43 44 45 46 47 48 49 4A 53 54 55 56	57
Blo	ock copy/overwrite Ctrl+W	y z f " + + * X Š ′ " " " • * " Š ¢ £ x ¥ ; 58 59 5A 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 9A A2 A3 A4 A5	A6
Blo	ck move Ctrl+M	E Ç Ž Ž Ž Č Ô Ô Ô Ö × Ø Ů Ú Á Á Ă Ă Ă Å x A A A A A A B A B B B B B B B B B B B	EA
Clin	- hand	U J • J J J J J J J J J J J J J J J J J	07
Cit	pooard	8 1 b r N T \$ 4 4 4 ñ 1 1 + 4 ' () + 5 6 7 61 71 13 22 32 81 08 14 42 91 A1 B1 C1 09 23 33 52 F0 15 62 72 D1 0A 16 24 34 E1 25 F1 17 18 19 1A 26 27 28 29 2A 35 36	37
Del	lete from cursor	YZ c d e f g h i j s t u v w x y z , f " + + 38 39 3A 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A 82 83 84 85 86	87
Del	lete to cursor	S - Θ = 4 3 / μ T · , 1 = λ λ λ λ λ E C Ž Ž Č Č Č Š 88 89 8A 92 93 94 95 96 97 98 99 9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2	D3
235101	ooxøuuaaaaçeee	🕫 ỗỗỗỗ ở 🛦 🗴 ỦỦ Ử 🗼 🖞 🚺 L 🕴 👌 🖞 🖞 L 5 D6 D7 D8 D9 DA E2 E3 E4 E5 E6 E7 E8 E9 EA F2 F3 F4 F5 F6 F7 F8 F9 FA FF C0 00 11 08 08 EE 05 FB 03 01 21 00 02 11	01
267 L	♦ y t □ L ¬ < L < 3	"PMHÅ ₁ Š @ / ₩ % 0 ₩ B 1 L 3 11 01 FF DA 00 0C 03 01 00 02 11 03 11 00 3F 00 84 50 4D 48 C5 02 8A 40 2F BD 25 30 13 BD 00 D0 02 66 93 9A 00 33 49	4C
290 J	SP ¥#0""Š`\$¶ (1	E Î Ž Å (+ § ¶ " D J (+ " P Ô " P Ô Å " + ' 04 A7 50 20 A5 A4 30 22 93 8A 60 25 14 00 B4 86 80 12 9E 05 28 10 A7 14 94 0C 4A 28 10 94 50 01 D2 94 50 00 D4 05 94 86	27
2B9 j.	J`¶₽ Kž+€ (Í!4	R P I 8 - 9 6 (CH D R 5 + 1 N 2 64 4A 60 14 50 01 4B 92 86 80 0A 28 00 CD 21 34 00 52 50 01 49 40 05 2D 00 14 EA 00 28 C7 BD 20 0C 52 E7 DE 81 87 7C D1	9E
2E2 h	9 J∖úó∔óIžh zó	P 1 Ô Ç Õ E 🛛 Å G Z J N Ô b - E ^l J = { P š 68 01 39 1F 4A 5C FA D3 10 D3 49 9E 68 01 7A D2 50 02 D2 E7 D6 80 0C F1 47 5A 00 4A 4E D4 00 62 96 80 03 4A 3D 7B 50 01	9A
30B J (С□ЪŠ`< · Zа4€)ЗІ	l 4 P Fh Ü 1 2 h Í Đ Í - * Ñ Í 4A 43 0C 62 8A 60 3C 87 1F 5A 61 34 80 29 33 4C 03 34 50 01 46 68 00 DC 69 32 68 00 CD 1C D0 01 CD 2D 00 1D BA D1 CD 00	19
334 >	Che j he pš pc	J 3 H a Š ; Đ À ÚĐ ਪ 2 3 8 - y P × ÖŠ 32 Å 6 8C F1 40 07 6Å 5C F1 40 09 DE 8Å 00 50 4F 4Å 33 48 61 9Å 38 D0 01 41 FA D0 01 9F 7Å 33 40 06 79 Å 0 50 01 D7 D6 8Å	00
35D ; 1	ŇÚEDÓE ₇ ŒzРŶ	s Jh ; Q Í ^L 9 Å ((é J) D) × :] 38 D1 DA 80 0C F3 45 00 02 8C 7A D0 01 C5 14 00 A0 73 4A 68 01 38 51 CD 03 0A 39 C5 00 28 E9 4A 29 0C 29 0D 00 19 A4 A6	02
386 f 1	KÞ ∂üé(ͥݩ((λΚ8• j λ λ - 'μ (6 λ ^J c ⁻ £ - / ? 83 4B DE 90 0B FC E9 28 18 BE DD λ9 28 01 28 λ0 41 4B 40 07 6λ 41 C5 00 2D 27 B5 00 28 E9 41 λ0 04 E7 λ8 λ3 λD 00 2F 3F	85
3AF (4 □ (úồ sĩJ (¤ •	¶ úB KÍ izt / " *ÅIÉÍ 28 34 0C 28 FA D2 01 73 EF 4A 28 00 A4 A0 05 07 14 A0 FA D0 01 4B CD 20 00 69 7A 74 A0 04 1E 94 B4 00 B9 C5 18 C9 CD 00	1D
3D8 @	GAÇÂİ <t¢ td="" åhzđ="" ž<=""><td>) v Š J . 1 f J + * # - 7 i e Ú * e C - A9 47 41 40 C3 18 3C 74 A2 90 08 48 7A D0 01 8E 29 76 8A 04 2E 31 CD 04 F7 A0 00 B9 23 AD 37 69 EB DA 98 0A 00 EB 43 0A</td><td>06</td></t¢>) v Š J . 1 f J + * # - 7 i e Ú * e C - A9 47 41 40 C3 18 3C 74 A2 90 08 48 7A D0 01 8E 29 76 8A 04 2E 31 CD 04 F7 A0 00 B9 23 AD 37 69 EB DA 98 0A 00 EB 43 0A	06
401 3	ŇŽh Ì¥ ◀@‡ži⊒g	4 " ! H 7 £ Ô E J E Y 3 H L H 6 33 1C D1 82 68 00 18 A5 1C 11 40 87 9E 69 08 E7 34 00 84 13 48 05 00 37 19 A3 1E D4 01 18 EB 4A 45 59 90 0A 33 48 03 BD	36
42A ~	leh Íex Jadier	â) a ô x 1 ^w µ 1 ¥ j Z J ^ Ô Q 8 Å Š 98 05 26 68 00 CD 26 78 A0 04 34 0E 69 80 B4 B9 E2 81 05 29 A0 61 F5 A4 A0 02 93 B5 02 0F 6A 5A 00 4A 5E D4 00 51 40 C2	8A
453 J	9 ″ ′ - 6 (ä@ I@• :	1 8 - 9 ¥ ^l · Z J (Å ¶ " bŠ C K 8 1) 04 14 94 00 B4 0A 06 25 28 EB 40 09 49 40 07 6A 31 40 06 39 A5 A0 03 B7 5A 4A 00 28 C5 00 14 94 00 62 BA 00 43 4B 40 08	29
47C Ý	"Il' bf-cžicae	ΧΨĴ d Đ ! 'z \sE ÎΨη 6 ÎQ & Š C Ŏ DD A8 00 CF 14 B9 A0 62 66 96 80 0F C6 8C E2 80 0F A5 04 64 D0 21 0D 27 7A 00 5C 73 45 00 18 A5 02 80 14 51 DF 8A 00 43	D6
4A5 "	¶ cŠ•Z ^Ô†Js(, E + 1 2 ((t¥Í ¶v 」Å 7 - 93 14 00 63 8A 07 5A 00 5E D4 86 81 85 04 73 40 82 8F C6 81 86 69 32 28 01 28 A0 00 74 A5 CD 00 14 76 A0 04 C5 18 A0 02	96
4CE € .	₿Ŭ£4 Q@ ¶ P:P B	9 3 3 0 1 2 Ú C ; P Fh + e C 2 h 80 0 E D 9 A 3 4 00 5 1 40 05 1 4 00 5 0 3 5 0 1 4 5 00 1 4 BD A 8 00 A 0 D 2 18 51 D A 80 0 A 38 50 0 1 4 6 6 8 00 F7 A 2 80 0 A 3 6 6	00
457 +	£µ¶;•èāµ ó:	~ " 🖸 2 }) 9 u Đ 1 a " 4 - 4 RāŽh F7 A3 B5 00 14 BF 95 00 1D E8 E3 B5 00 00 F3 4A 7E 94 0C 32 7D 29 39 A0 00 75 A0 D0 02 E6 93 BD 00 2D 25 00 00 52 E3 BE	68
520 T) 1 " C C - ; x 4 ~ £ ;	9 18 3 5 + ; DE I 1 1 f 8 3 I C B (18 9D 29 69 00 B9 A2 80 17 A1 A4 34 00 98 A3 B5 00 14 01 EF 40 0B F5 A0 1A 00 3B D0 45 00 18 EF 49 83 40 0B 49 C7 42 28	01 🚽
Adr. dec: 0	Char dec: 255 Overwrite	elete from begin until current adress (incl.)	
@ (2 🖉 🔚		AM 917



Assessment Hints

The ASCII view of the data (file) received from the session. Note the file signature GIF89a

Wireshark · Follow TCP Stream (tcp.stream eq 2) · rhino2	-		\times
HTTP/1.1 200 OK Date: Wed, 28 Apr 2004 21:07:34 GMT Server: Apache/1.3.29 (Unix) Last-Modified: Wed, 28 Apr 2004 21:07:34 GMT ETag: W/"19b1e7-14c91-40901d9c" Accept-Ranges: bytes Content-Length: 85137 Keep-Alive: timeout=15, max=99 Connection: Keep-Alive Content-Type: image/gif			^
GIF89a IG8 54.45.6n.66?cd5V.& [doE56.?4.E?.56k.Fu5>n\4.4.`#A?.?@.MT.2 #?t.DcL j. dxV.:/Jt6:.a0oL.1.) .'2K. 85h88\$J 5B.T;o	n	 jw	
<pre>2]<+).1.S6A\.qd\$0>ug.de/d.!.TJ.2 5j.R.i 4.VHcuJHPZ.Lk.uLk>r+KX."~.*90.6(d%Ch.().\$.W.L:1JHn.)I.QG.C.k,[u.av:\$2p.W1N0d! R*<cpre>cE.)G F&@Hr \. .W*.BHV.8YC\$r."].e~Ld v1.Qi5YiX > ; XA}4@.&QUPD8`Me7K+Att.]</cpre></pre>	•.@t.x.	C%?h	
7KD.:.zSc.P.)1.0S)&.Z0 ^pe.,~E.V5E 80% L.&yE.1QaDA.3I7I7LKwm7.L.3mY +C.P.s5be@.Snp.@U'' <hh.s` 4 chent pkts, 63 server pkts, 5 turns.</hh.s` 			~
Entire conversation (86 kB)		Stream 2 Find <u>N</u> e	÷ ext
Filter Out This Stream Print Save as Back Cl	lose	Help	

The picture recovered for assessment (rhino5.gif)

