



Where serious technology buyers decide

Network Forensics

Tracking Hackers Through Cyberspace

Sherri Davidoff and Jonathan Ham

Once Upon a Time...

- Hard drive forensics
- Useful, but:
 - You can't trust a compromised host
 - Limited space for logs
 - Just a small piece of the puzzle
- Like an autopsy of a body at a crime scene



Image: http://commons.wikimedia.org/wiki/File:Hdd-serial_ata.jpg

Now: Network Forensics

- The rest of the crime scene
 - Footprints, fingerprints, bullets in the wall
- Firewalls
- Web proxies
- DHCP servers
- Central log servers
- Flow records
- Traffic on the wire (or in the air)

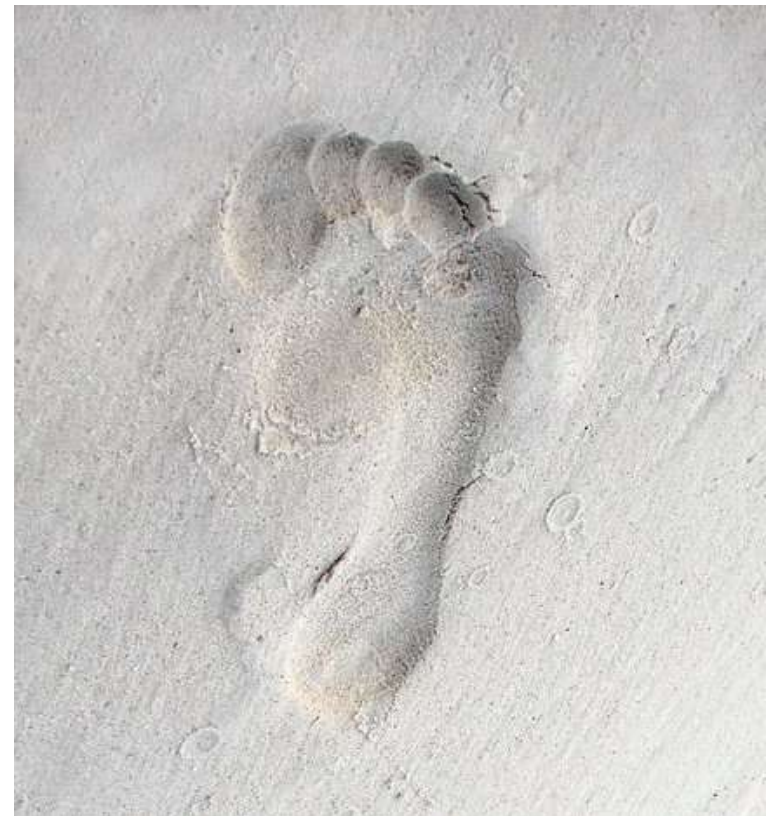


Image: Nevit Dilmen, http://commons.wikimedia.org/wiki/File:Maldives_00147_foot_print_on_earth.jpg

Catch a Brute Force Attack – Flow Records

- Successful brute force attack
- Regular automated attempts (every 2 seconds)
- Followed by large data transfer

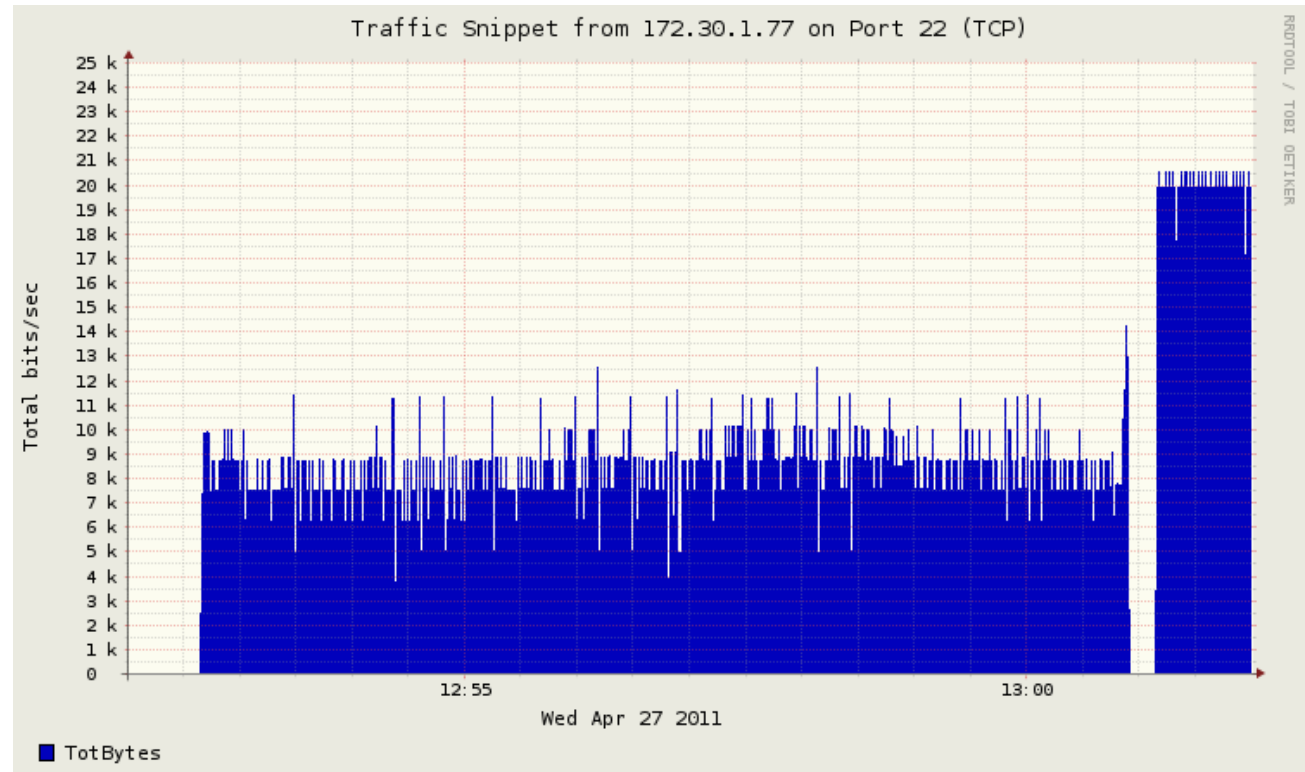


Image: Copyright LMG Security, 2011. Used with permission.

From “Network Forensics” (ch. 5) – Day 1 of the Black Hat class

Brute Force – Event Logs in Splunk

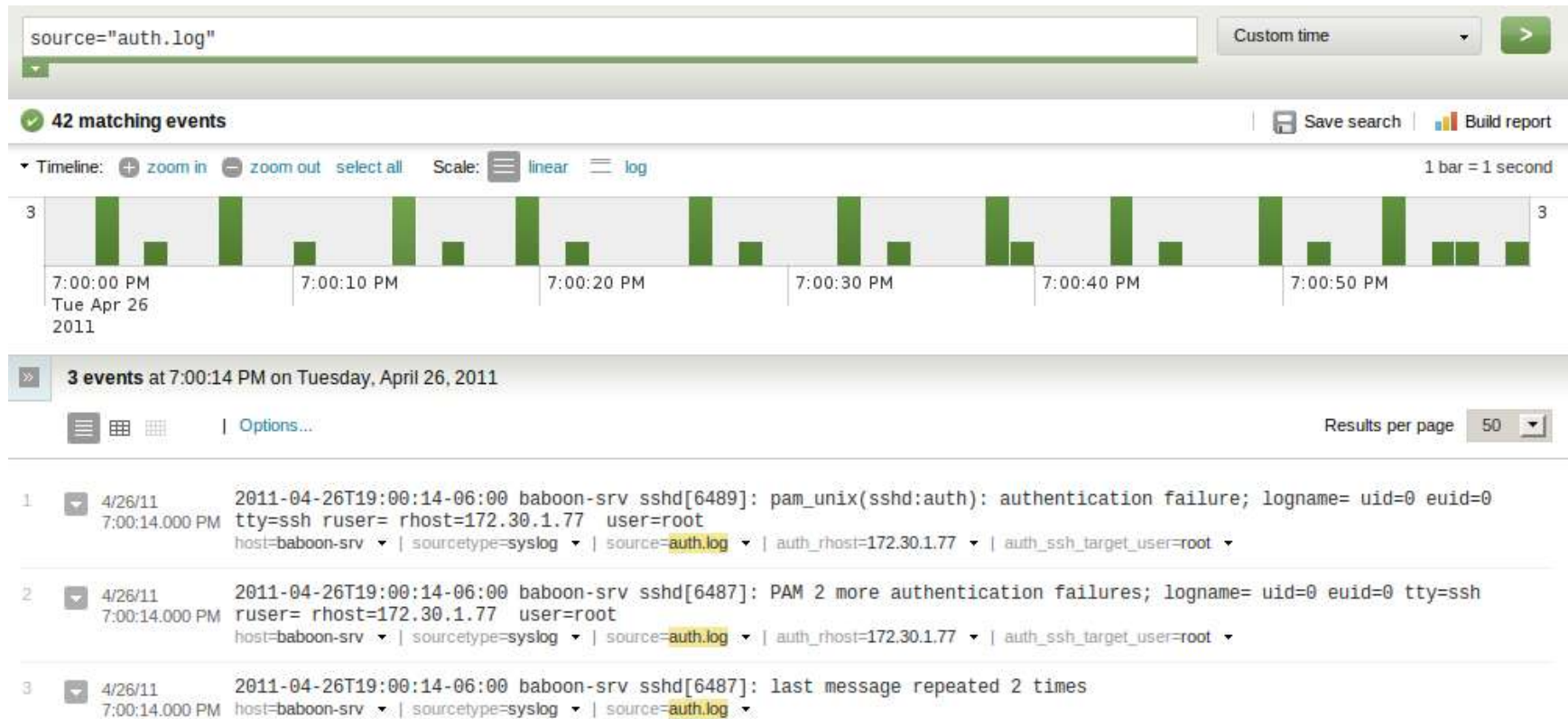


Image: Copyright LMG Security, 2011. Used with permission.

From “Network Forensics” (ch. 8)

Brute Force – Targeted Accounts in Splunk

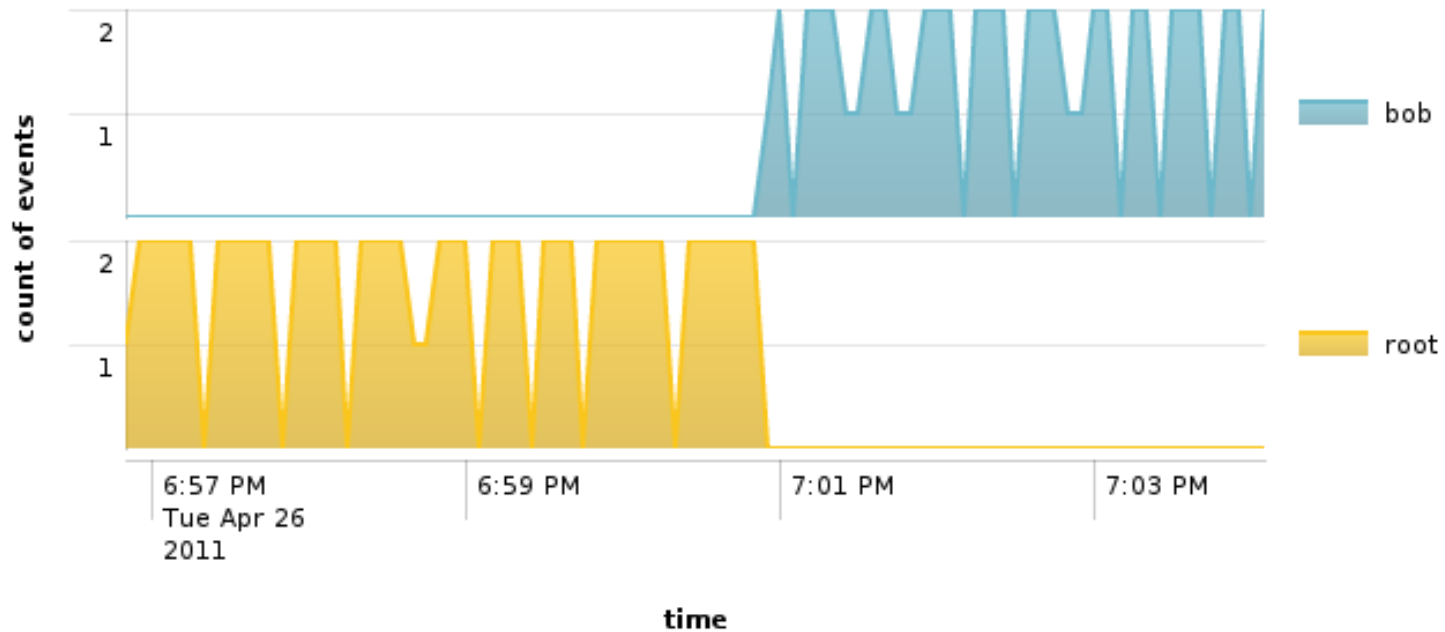
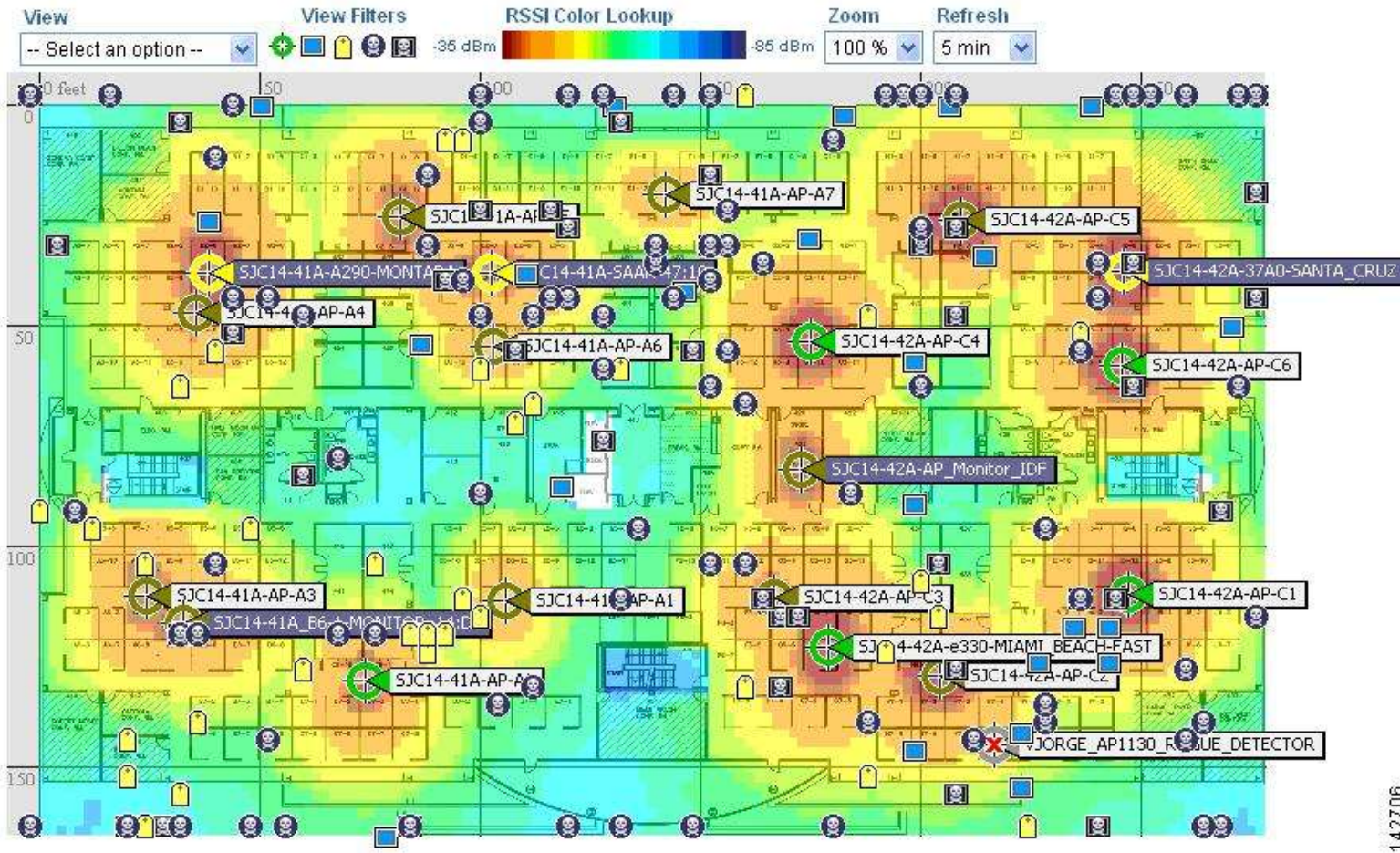


Image: Copyright LMG Security, 2011. Used with permission.

From “Network Forensics” (ch. 8)

Wireless – Track Down Rogue Laptops



142706

Image: Copyright Cisco Systems, 2011.

From “Network Forensics” (ch. 6) – Day 2 of the Black Hat class

Web Proxies – Browsing Histories for Everyone



Squid User Access Reports

Period: 2011May18-2011May18

User: 192.168.1.170

Sort: BYTES, reverse

User Report

ACCESSED SITE	CONNECT	BYTES	% BYTES	IN-CACHE	OUT	ELAPSED TIME	MILISEC	% TIME
www.boingboing.net	72	2.64M	21.25%	4.44%	95.56%	00:00:51	51,118	10.06%
safebrowsing-cache.google.com	19	2.54M	20.44%	0.00%	100.00%	00:00:10	10,823	2.13%
a.fsdn.com	41	1.31M	10.57%	60.33%	39.67%	00:00:07	7,210	1.42%
threatpost.com	71	782.52K	6.29%	2.90%	97.10%	00:00:18	18,476	3.64%
boingboing.net	27	693.88K	5.58%	45.63%	54.37%	00:00:09	9,721	1.91%
s0.2.mdn.net	21	555.72K	4.47%	0.23%	99.77%	00:00:03	3,730	0.73%
craphound.com	14	502.73K	4.04%	0.00%	100.00%	00:00:13	13,145	2.59%
news.discovery.com	31	313.73K	2.52%	0.00%	100.00%	00:00:05	5,712	1.12%
www.computerworld.com	68	287.21K	2.31%	12.50%	87.50%	00:00:08	8,926	1.76%
science.slashdot.org	4	252.68K	2.03%	25.58%	74.42%	00:00:02	2,504	0.49%
www.kqed.org	48	172.90K	1.39%	3.09%	96.91%	00:00:16	16,320	3.21%
lakemissoulagroup.com	27	169.10K	1.36%	0.00%	100.00%	00:00:02	2,667	0.52%
s.ytimg.com	8	161.27K	1.30%	66.55%	33.45%	00:00:00	800	0.16%
tech.slashdot.org	2	133.19K	1.07%	0.00%	100.00%	00:00:01	1,220	0.24%
hardware.slashdot.org	2	126.66K	1.02%	0.00%	100.00%	00:00:01	1,541	0.30%
pagead2.google syndication.com	9	126.35K	1.02%	23.44%	76.56%	00:00:00	920	0.18%

Image: Copyright LMG Security, 2011. Used with permission.

From “Network Forensics” (ch. 10) – Day 3 of the Black Hat class

Carving a JPG Out of a Web Proxy Cache

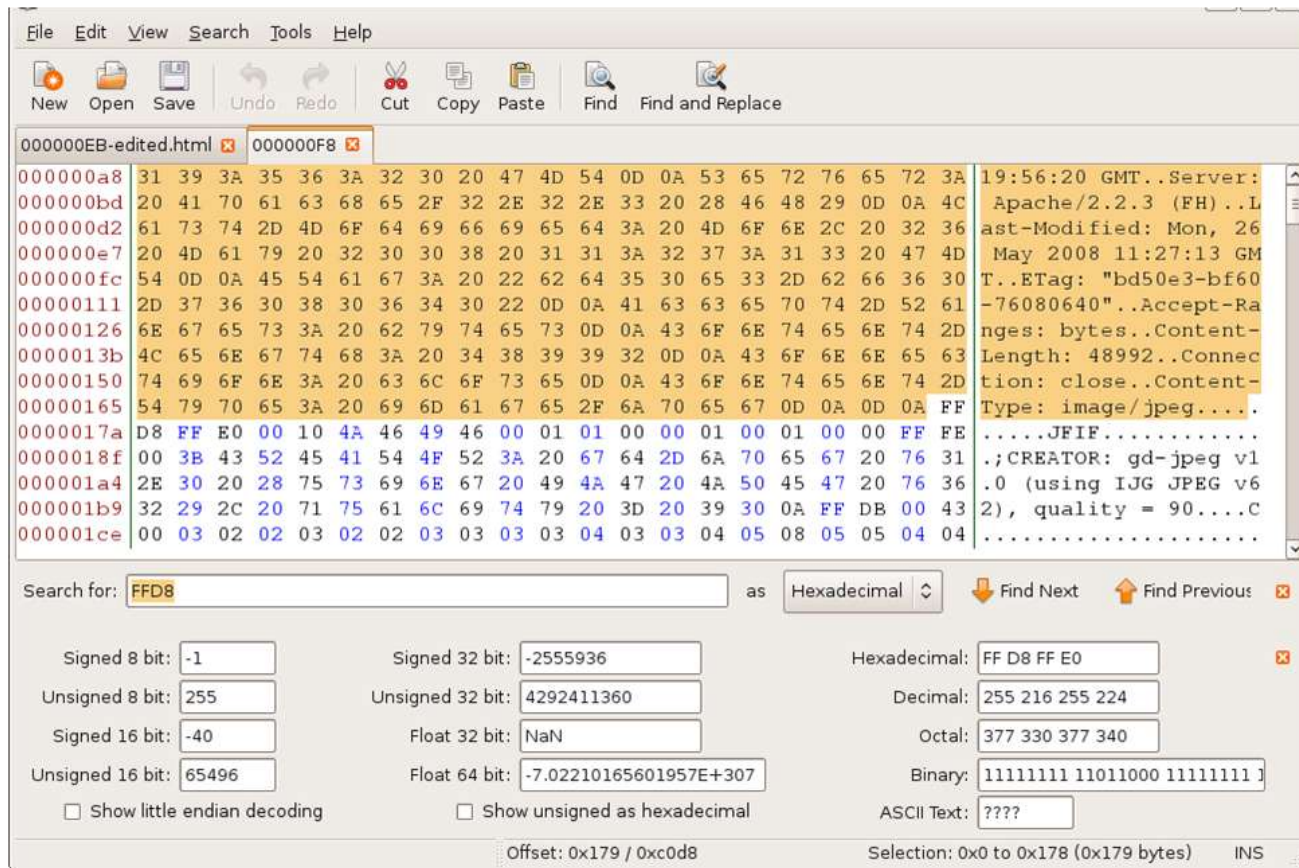


Image: Copyright LMG Security, 2011. Used with permission.

From "Network Forensics" (ch. 10) – Day 3 of the Black Hat class

Carving a JPG Out of a Web Proxy Cache



Image: Copyright LMG Security, 2011. Used with permission.

From "Network Forensics" (ch. 10) – Day 3 of the Black Hat class

Malware – Metasploit in Network Traffic

The screenshot shows a network traffic analysis interface. At the top, there is a filter section with a dropdown menu set to 'Expression...', and buttons for 'Clear' and 'Apply'. Below this is a table of network traffic entries. The table has columns for 'No.', 'Time', 'Source', 'Destination', 'Protocol', and 'Info'. Several entries are highlighted in red, indicating a filter is applied. The highlighted entries show TCP connections from 10.10.10.10 to 10.10.10.70. The 'Info' column for these entries includes details like '[TCP Port numbers reused]', '4445 > 1044 [RST, ACK] Seq=197', and '1044 > 4445 [SYN] Seq=197'. Below the table, there is a section for 'Data (1460 bytes)' with a hex dump and its corresponding ASCII representation. The ASCII representation shows a Metasploit payload: '.L!This program cannot be run i n DOS mo de...\$.'. The hex dump shows the raw bytes of the payload, including the 'MZ' signature at the beginning.

No. -	Time	Source	Destination	Protocol	Info
1652	2010-04-28 17:42:02.001752	10.10.10.70	10.10.10.10	TCP	[TCP Port numbers reused]
1653	2010-04-28 17:42:02.001815	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [RST, ACK] Seq=197
1654	2010-04-28 17:42:02.548001	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [SYN] Seq=197
1655	2010-04-28 17:42:02.548065	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [RST, ACK] Seq=197
1656	2010-04-28 17:42:02.985483	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [SYN] Seq=197
1657	2010-04-28 17:42:02.985580	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [SYN, ACK] Seq=197
1658	2010-04-28 17:42:02.985870	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [ACK] Seq=197
1659	2010-04-28 17:42:03.217075	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [PSH, ACK] Seq=197
1660	2010-04-28 17:42:03.220699	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [ACK] Seq=143
1661	2010-04-28 17:42:03.220800	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [ACK] Seq=143
1662	2010-04-28 17:42:03.221154	10.10.10.70	10.10.10.10	TCP	1044 > 4445 [ACK] Seq=197
1663	2010-04-28 17:42:03.221372	10.10.10.10	10.10.10.70	TCP	4445 > 1044 [ACK] Seq=143

Window size: 5840
▶ Checksum: 0x0730 [correct]
▶ [SEQ/ACK analysis]
▼ Data (1460 bytes)
Data: 4D5AE8000000005B52455589E581C3CB110000FFD389C357...
[Length: 1460]

```
0030 16 d0 07 30 00 00 4d 5a e8 00 00 00 00 5b 52 45 ...0..MZ ....[RE
0040 55 89 e5 81 c3 cb 11 00 00 ff d3 89 c3 57 68 04 U..... ..wh.
0050 00 00 00 50 ff d0 68 f0 b5 a2 56 68 05 00 00 00 ..P..h. ..vh....
0060 50 ff d3 00 00 00 00 00 00 00 00 00 00 00 00 P..... ..
0070 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 ..!..... ..!
0080 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d .L!This program
0090 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 cannot be run i
00a0 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0a 24 00 n DOS mo de...$.
00b0 00 00 00 00 00 00 8a e2 9d d8 ce 83 f3 8b ce 83 ..
00c0 f3 8b ce 83 f3 8b c7 fb 77 8b e4 83 f3 8b c7 fb ..
00d0 66 8b d3 82 f2 8b ce 82 f2 8b 66 82 f2 8b ce 45 f.....f..f..
```

Image: Copyright LMG Security, 2011. Used with permission.

From “Network Forensics” (ch. 12) – Day 4 of the Black Hat class

Malware – Bad Bad JavaScript

The image shows a Wireshark network traffic capture. The filter is set to `(ip.addr == 10.10.10.70) && (ip.addr == 10.10.10.10)`. The selected packet is No. 11, a GET request for `/index.phpmFKSxSANkeTeNrah.gif`. The packet details show the following JavaScript code:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN">\n<html>\n<head>\n<script>\nvar UwnHADofYHiHDDXj = "COMMENT";\nvar qSngVkOrdIjaiFpPTfDjbPHQppHSGTzpm00yqEbLEFxnqAxicRyZKKwiRwmUaDHFouzHPHqLrRFSzQuPusTnQyqpQwVpARdLR = new Array();\nfor (i = 0; i < 1300; i++)\n{\n  qSngVkOrdIjaiFpPTfDjbPHQppHSGTzpm00yqEbLEFxnqAxicRyZKKwiRwmUaDHFouzHPHqLrRFSzQuPusTnQyqpQwVpARdLR[i] = document.createElement(UwnHADofYHiHDDXj);\n  qSngVkOrdIjaiFpPTfDjbPHQppHSGTzpm00yqEbLEFxnqAxicRyZKKwiRwmUaDHFouzHPHqLrRFSzQuPusTnQyqpQwVpARdLR[i].data = "vEI";\n}\n
```

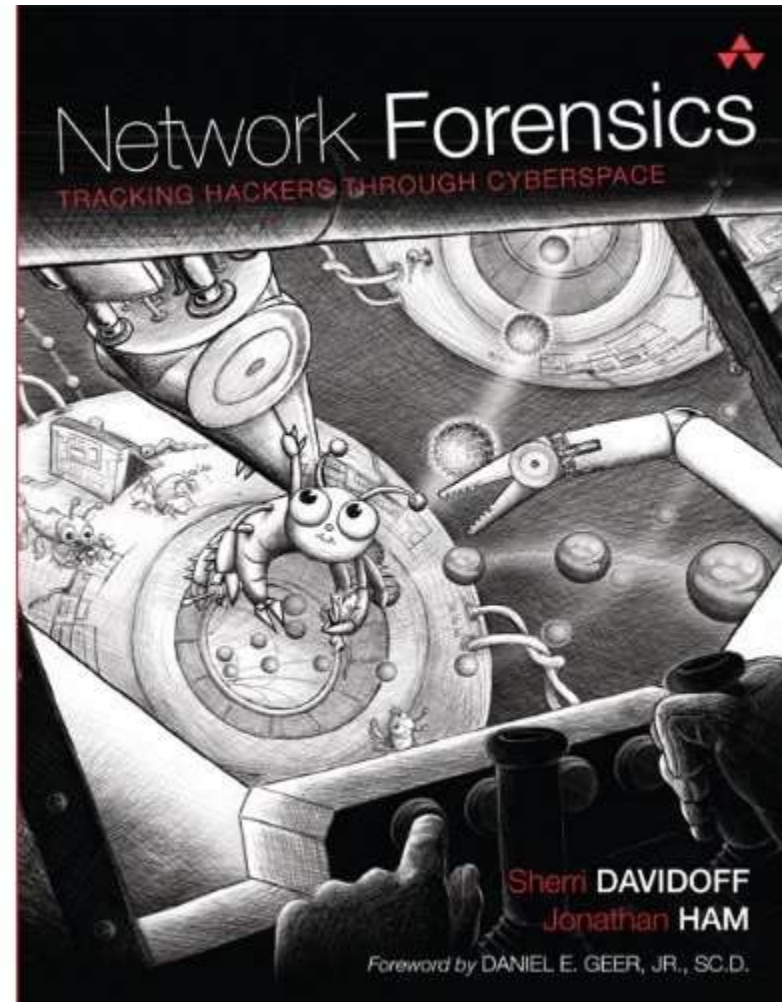
The packet bytes pane shows the raw data of the JavaScript code, with the first few bytes being `<!DOCTYPE HTML PUBLIC`.

From “Network Forensics” (ch. 12) – Day 4 of the Black Hat class

'Network Forensics'

- The book!
 - Brand new material
 - Released next week
- Also: Join us at Black Hat
 - 4-day intensive class
 - Taught by the authors
 - *Network Forensics: Black Hat Release*
 - July 21-24
 - Register today!

<http://NetForensicsClass.com>



Questions?

Send them to Sherri and Jonathan via the text chat area on the left

- Select "Presenters" to submit your question privately*
- We'll answer as many as we can!*

The speakers:

Sherri Davidoff & Jonathan Ham

- sherri@imgsecurity.com

- jonathan@imgsecurity.com

**Join us at Network Forensics:
Black Hat Release (July 21-24)**

- <http://NetForensicsClass.com>

