TechTarget

Where serious technology buyers decide

Network Forensics

Tracking Hackers Through Cyberspace

Sherri Davidoff and Jonathan Ham

© TechTarget

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

© TechTarget

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

© TechTarget

Catch a Brute Force Attack – Flow Records

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

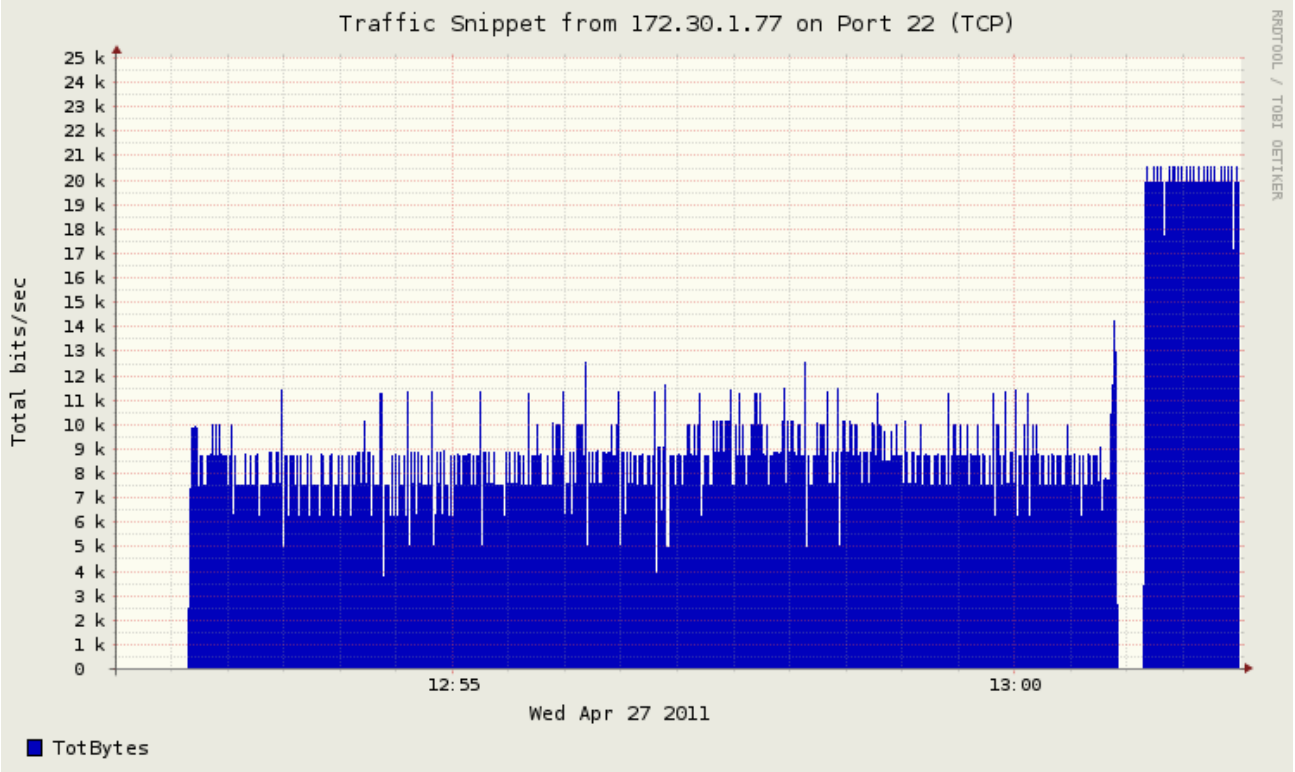


Image: Copyright LMG Security, 2011. Used with permission.

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

© TechTarget

Brute Force – Event Logs in Splunk

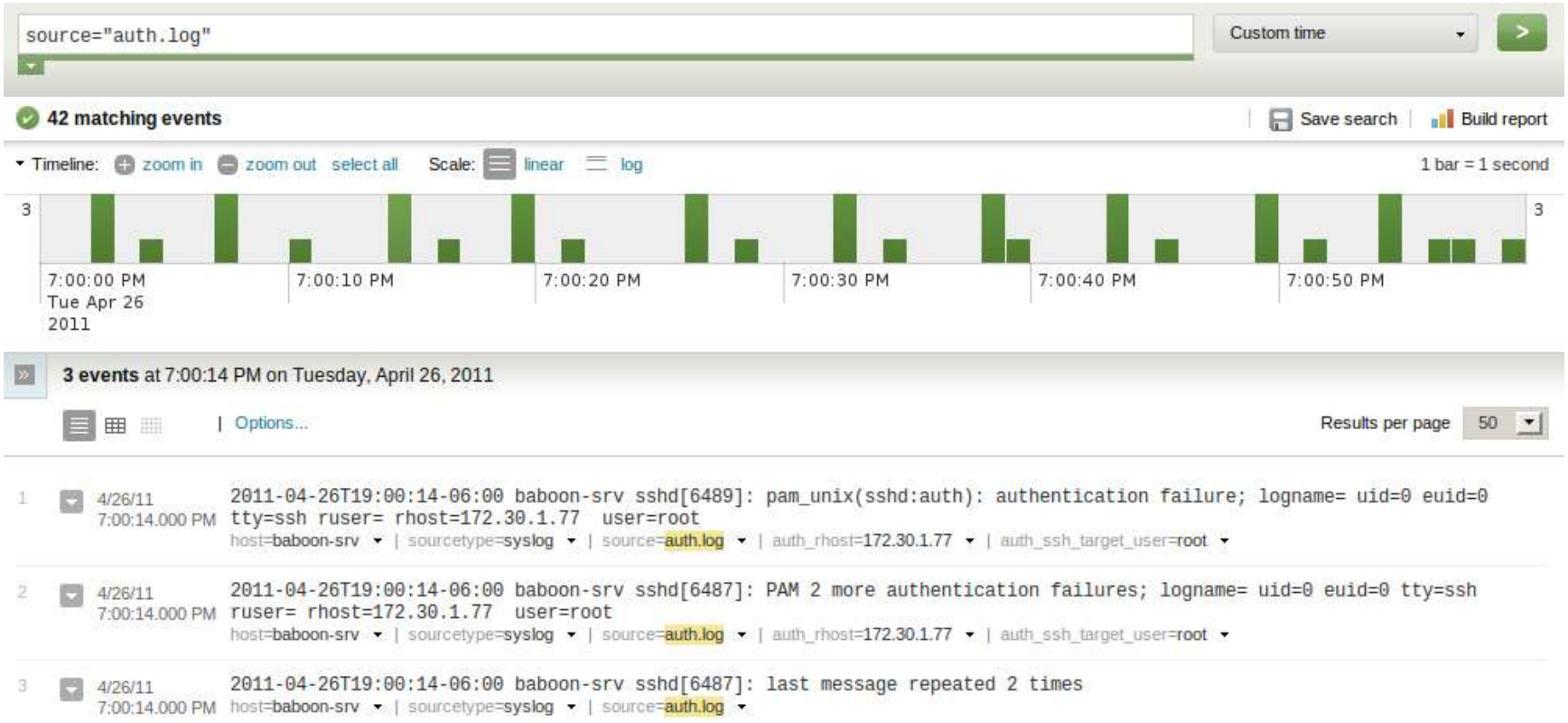


Image: Copyright LMG Security, 2011. Used with permission.

From “Network Forensics” (ch. 8)

© TechTarget

Brute Force – Targeted Accounts in Splunk

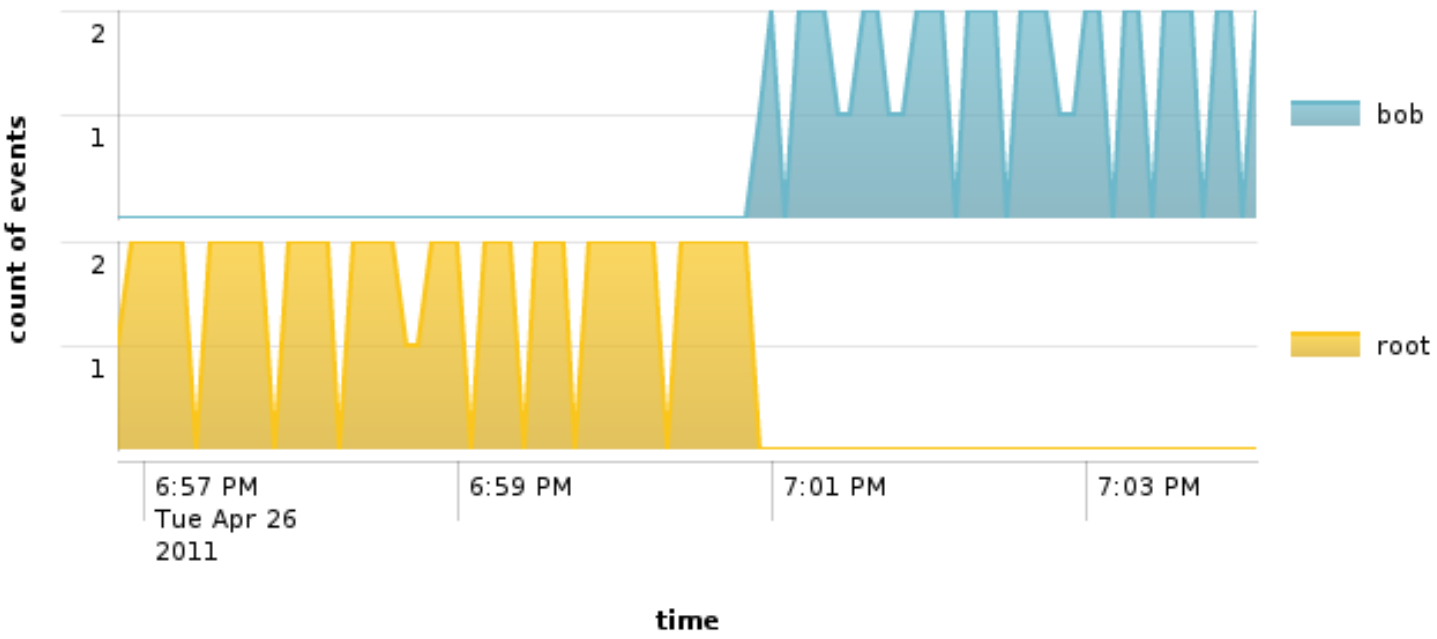


Image: Copyright LMG Security, 2011. Used with permission.

From “Network Forensics” (ch. 8)

© TechTarget

Wireless – Track Down Rogue Laptops

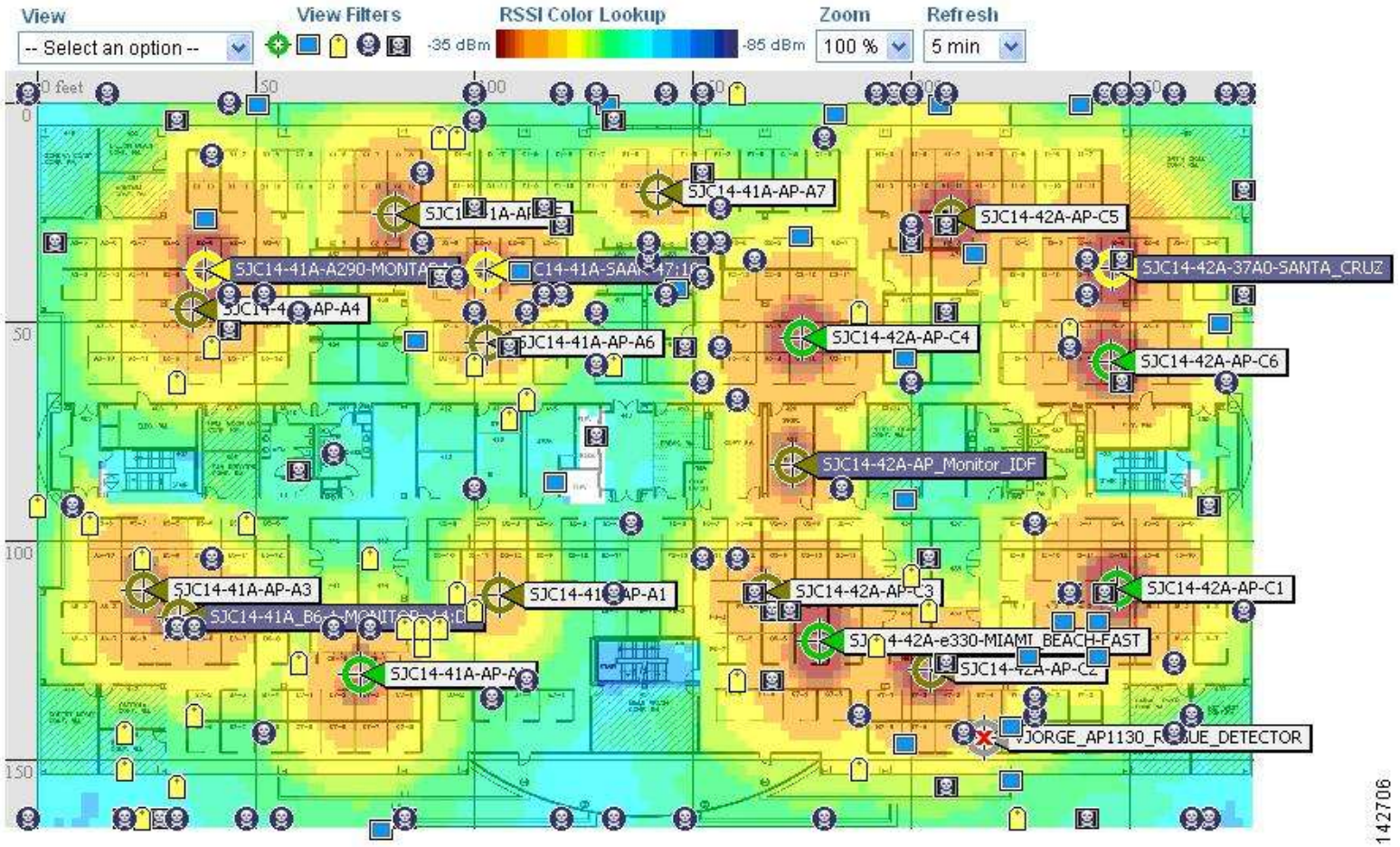
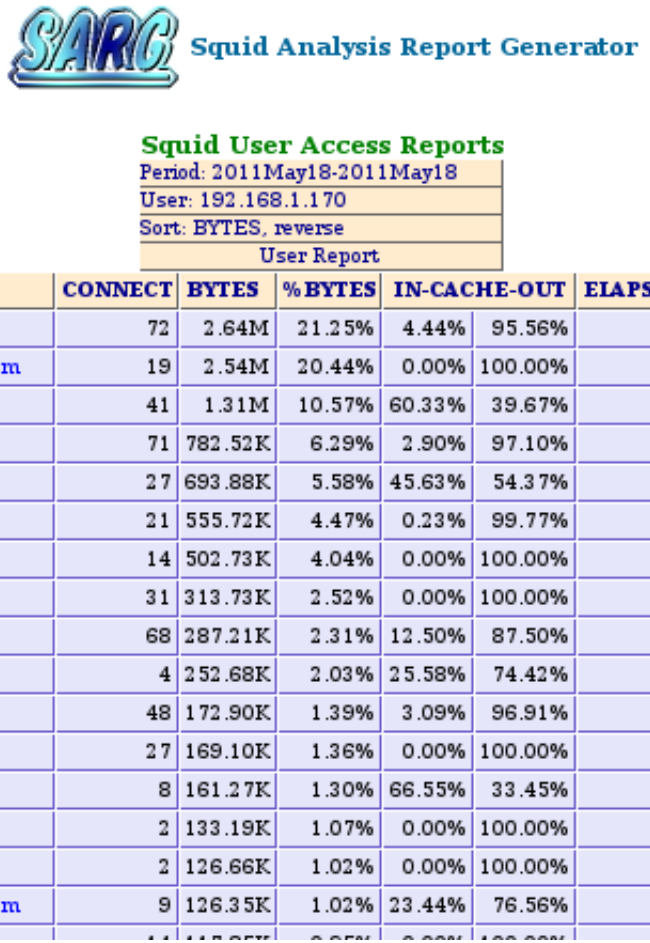


Image: Copyright Cisco.Systems, 2011.

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

Web Proxies – Browsing Histories for Everyone



SARG Squid Analysis Report Generator

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%
s0.2mdn.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.googlesyndication.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

© TechTarget

Carving a JPG Out of a Web Proxy Cache

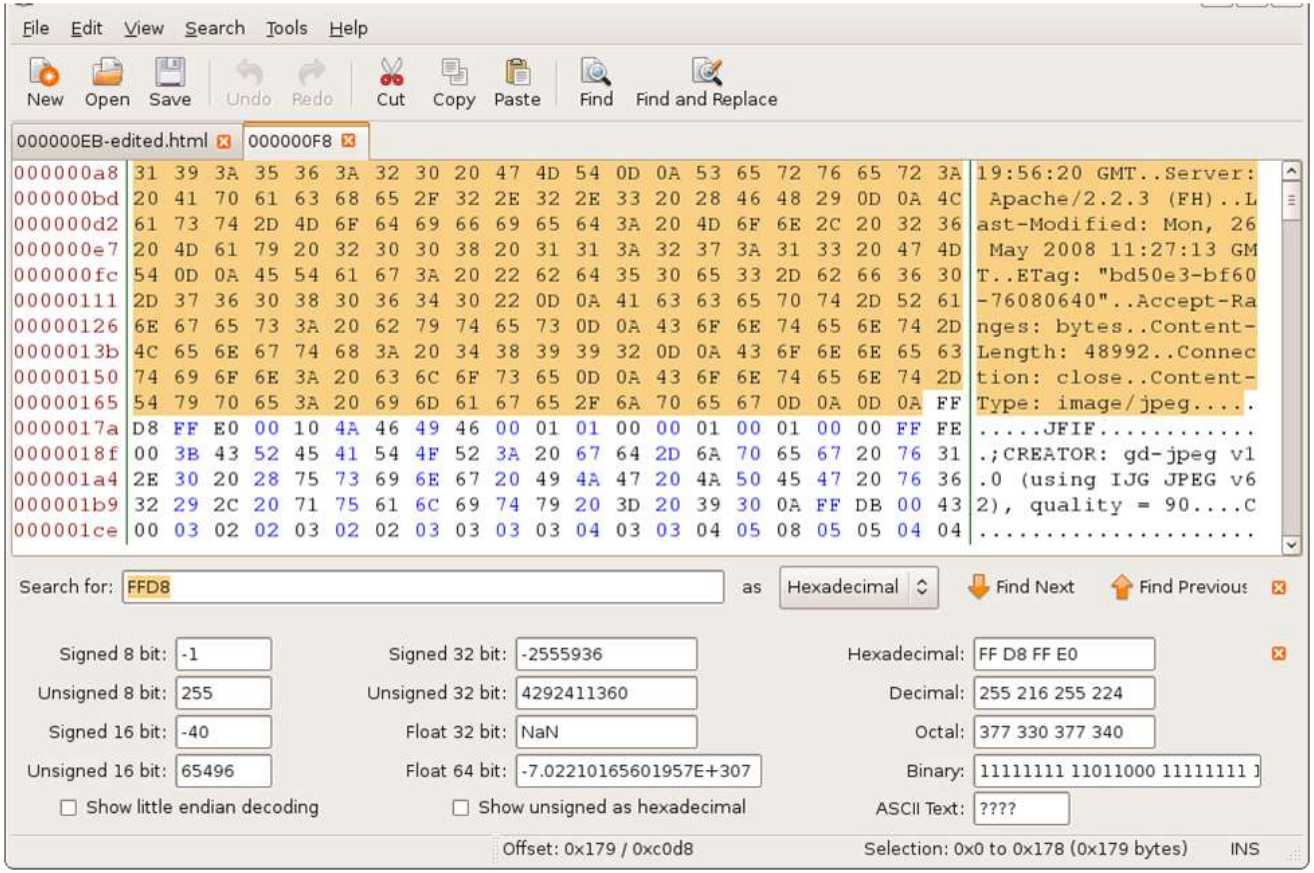


Image: Copyright LMG Security, 2011. Used with permission.

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

© TechTarget

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

© TechTarget

Malware – Metasploit in Network Traffic

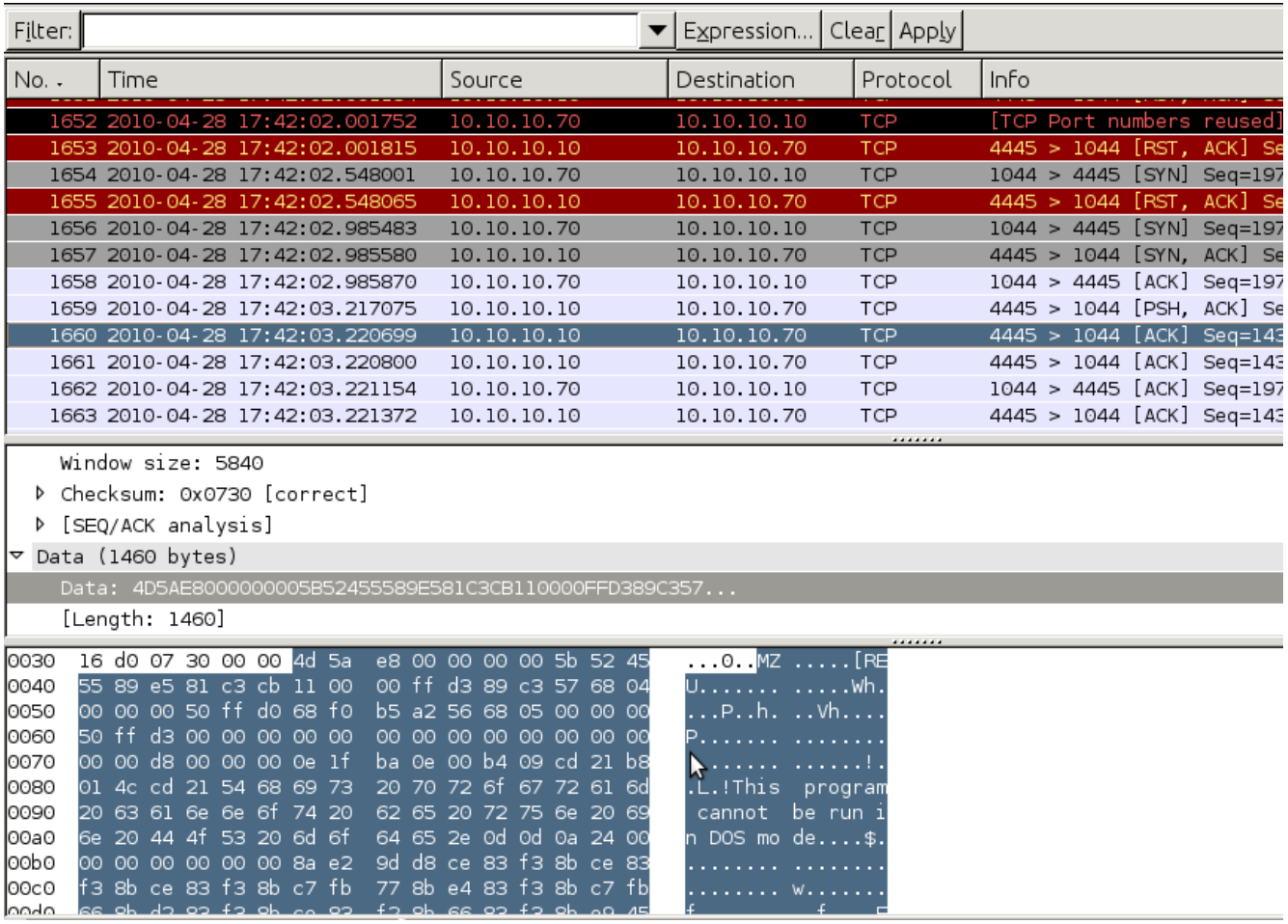
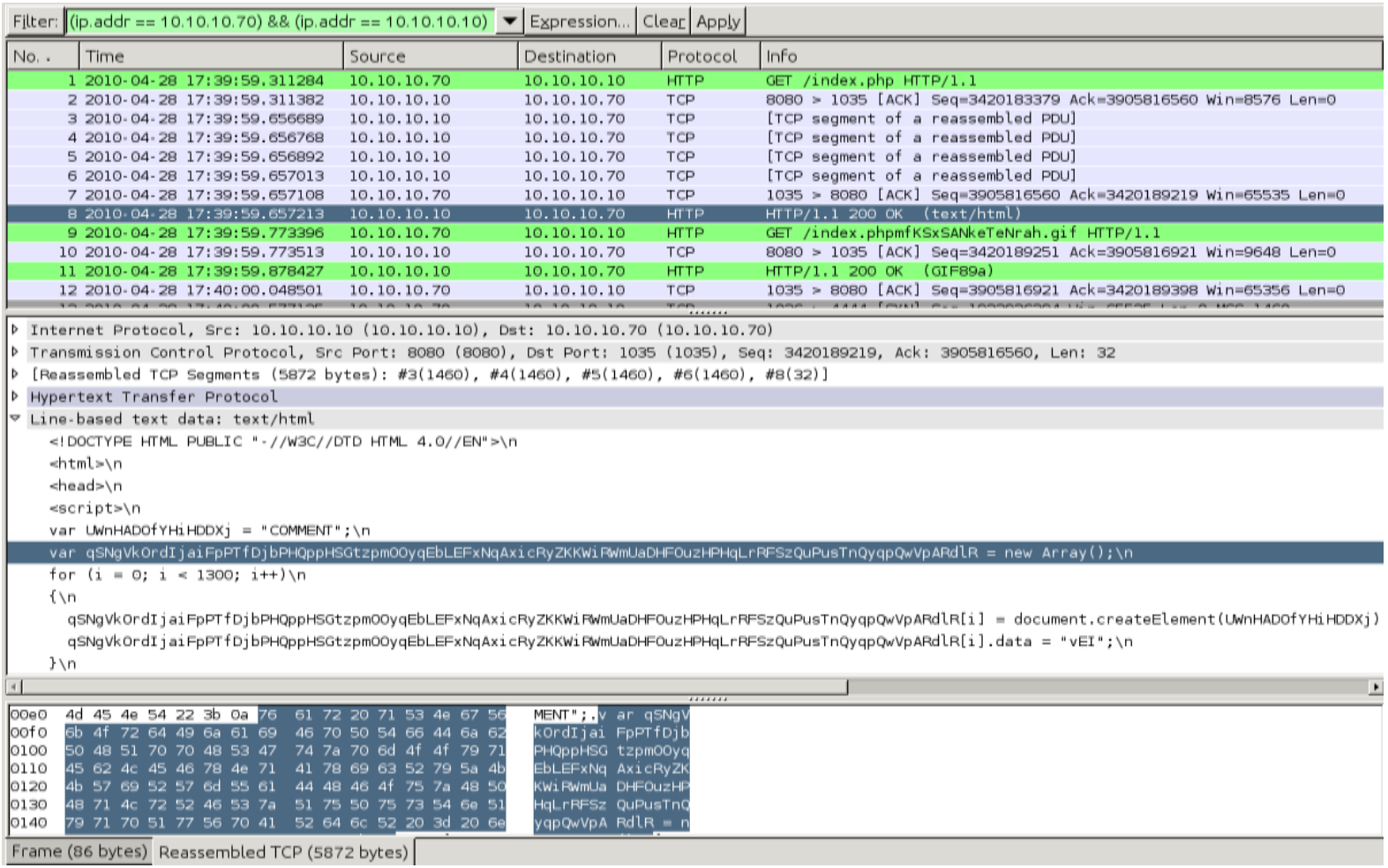


Image: Copyright LMG Security, 2011. Used with permission.

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

© TechTarget

Malware – Bad Bad JavaScript



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

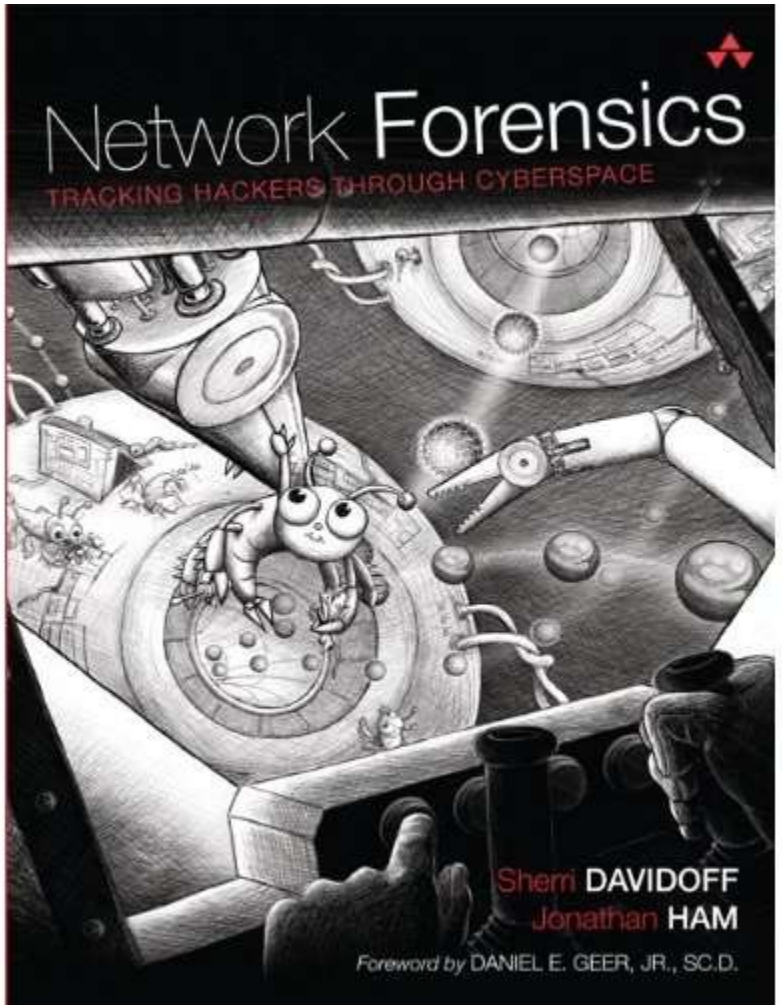
© TechTarget

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

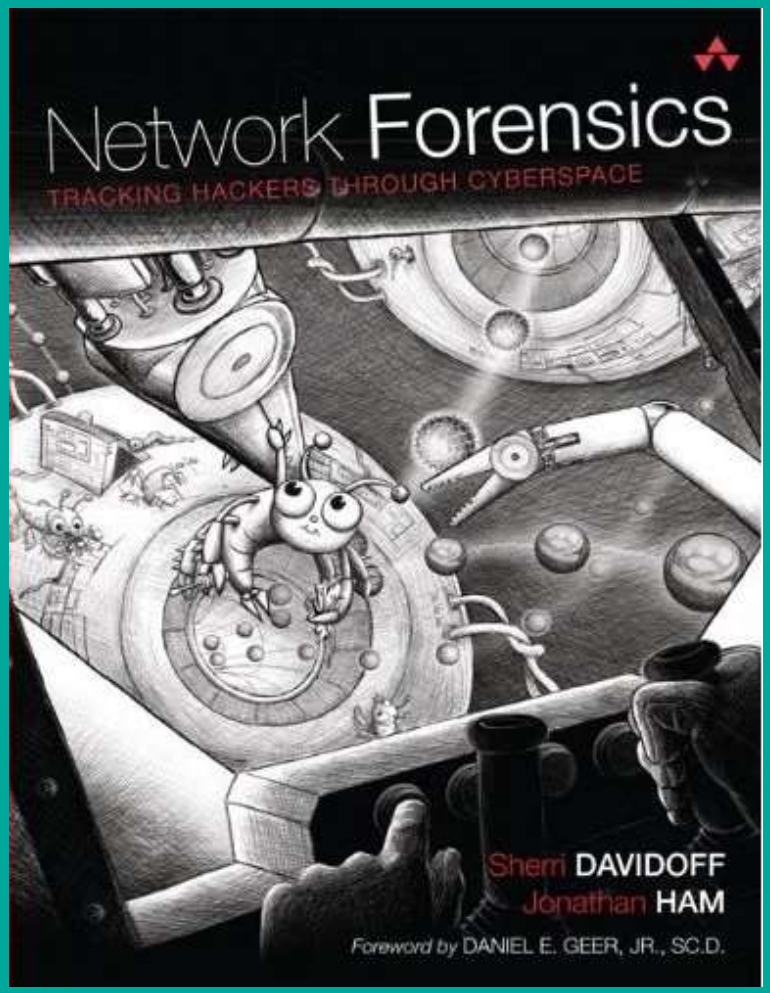
‘Network Forensics’

- 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



© TechTarget



TechTarget

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@lmgsecurity.com***
- ***jonathan@lmgsecurity.com***

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

- **http://NetForensicsClass.com**

© TechTarget