HERIOT WATT UNIVERSITY

BSc Cyber Security

F20FO

Digital Forensics

Coursework Two

By Fatima HanifMohammed Patel

H00339652 fp17@hw.ac.uk

Forensic Images Link: F20FO_CW2_Forensic_Images

Table of Contents

1 Introduction

This report covers the process of creating a forensically sound image of the provided digital evidence and analyzing it using various tools with different purposes to extract various kinds of information. The provided evidence consisted of the primary descriptor file for the virtual machine (Lubuntu 64-bit.vmdk) which contains metadata about the configuration of the virtual disk and points to the other split virtual disk files of the virtual machine (Lubuntu 64-bit-s00X.vmdk). These files contain the actual data of the VM's hard drive, including the operating system, installed applications, and user data. Lubuntu 64-bit.nvram stores the state of the VM's BIOS. Lubuntu 64-bit.vmx is the primary configuration file for the virtual machine. It contains settings like CPU allocation, memory size, and the hardware configurations of the VM. Lubuntu 64-bit.vmxf is a supplemental configuration file that stores additional settings for the VM. It's used alongside the .vmx file. Lubuntu 64-bit.vmsd stores metadata and information about snapshots of the VM. In this case, it's empty (0 bytes), indicating there are no snapshots.

Because of ACPO Principle 1, the first step is to image the provided virtual machine before analysis [1].

2 Imaging

Forensic imaging is not just creating a file copy of the digital evidence since copies do not recover all data areas of the device for examination. Working from a duplicate image preserves the original evidence, prevents inadvertent alteration of original evidence during examination and allows recreation of the duplicate image if necessary [2]. The utilization of multiple specialized forensic imaging tools is advantageous because each tool may have unique features. For instance, FTK Imager is renowned for its user-friendly interface and comprehensive imaging capabilities, while tools like dd offer powerful command-line options for creating raw images.

3.1 Imaging using FTK

Various image formats are available in Forensic Toolkit (FTK) catering to different needs and scenarios in digital forensic investigations. Two popular image formats will be used in this investigation, expert witness format and raw dump.

The Expert Witness Format includes a header with case and acquisition information, organizes data into blocks of 64 sectors (32 KB each) with a CRC check for each block, and concludes with an acquisition hash for integrity verification [3]. Additionally, it supports lossless compression and password protection of digital forensic images (DFIs) [3].

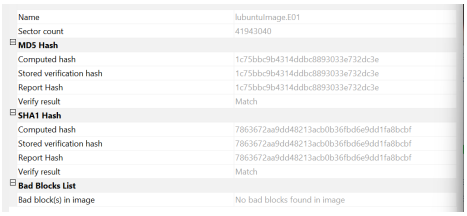


Figure 1 Integrity Check of Image

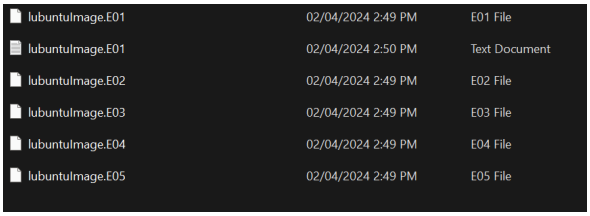


Figure 2 Image Files

Raw (DD) format creates a bit-for-bit copy of the evidence without any metadata about the imaging process [3]. Its simplicity and compatibility make it widely used, but the lack of metadata means that information about the imaging process must be documented separately. FTK does provide an integrity check for raw dump formats of evidence:

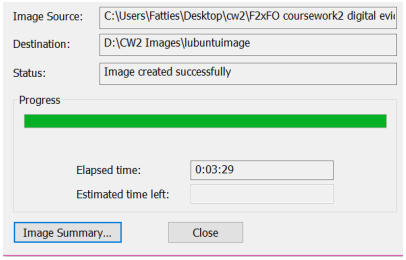


Figure 3 Creating Image

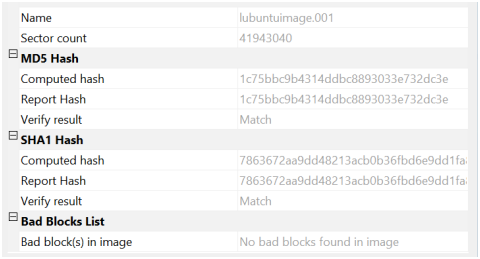


Figure 4 Inbuilt Integrity Check

3.2 Imaging using Data Dump (dd) – Linux CLI Utility

This is a bit-by-bit copy of the evidence and offers many advantages such as fast data transfer, simple to work with (only 1 CLI command) and most tools can work with raw formats. The disadvanages include requiring as much storage as the original data and validation check must be done seperately [4]. For this investigation, the signature of the original evidence was found, then after imaging using dd, the signature of the image was found. As shown below, the hashes match and therefore the integrity of the evidence is upheld:

```
seed@seed:~/john/run$ sha256sum ~/Desktop/shared/'F2xFO coursework2 digital evidence.zip'
27f6b33fb1465dd08f9d663fc6af0d6a29dc55a47fb63b99b40a172b12e470c9  /home/seed/Desktop/shared/F2xFO coursework2 digital evidence.zip

seed@seed:~/john/run$ dd if=~/Desktop/shared/'F2xFO coursework2 digital evidence.zip' of=~/Desktop/shared/cw2dd bs=4M status=progre
ss
7361003520 bytes (7.4 GB, 6.9 GiB) copied, 185 s, 39.8 MB/s
1755+1 records in
1755+1 records out
7362035398 bytes (7.4 GB, 6.9 GiB) copied, 185.089 s, 39.8 MB/s
seed@seed:~/john/run$ sha256sum ~/Desktop/shared/cw2dd
27f6b33fb1465dd08f9d663fc6af0d6a29dc55a47fb63b99b40a172b12e470c9  /home/seed/Desktop/shared/cw2dd
```

Figure 5 Data Dump and Integrity Check of Evidence

In conclusion, imaging using FTK is good for splitting the evidence into partitions, built in integrity check, choosing compression ratio, encryption and it supports 5 image formats. Were as, dd is good since it requires only one step, no additional applications must be installed since it is a Linux utility and even if the evidence is not in a recognizable format, since it is simply a bit-by-bit copy, there are no issues. However, integrity check must be done separately for dd. These image files are what will be analysed in the next sections.

3 Analysis

3.1 Analysis using Autopsy

6 users found in home/: student1, student2, tutor1, user_one, user_ten and f21fo-cw2. The first 5 users were created on the same day within 5 minutes. Only user f21fo-cw2 has files associated with them.

In **media/f21fo-cw2** a deleted folder called ***RYAD SIGS*** was found.

Documents include: Folders about astronomy, blackholes, stars, astronomers, solar system and digital forensics.

Audio

Music files with random audio: zipper, phone vibrating, bad violin, coughing, laughter, beats and more.

Pictures

Multiple pictures of the same candy and nuts and empty black tea cup. Upon inspecting the EXIF tags, it appears different cameras such as KODAK, NIKON D200, Panasonic DMC-FZ50 Ver.1.0, OLYMPUS DIGITAL CAMERA, Samsung VLUU L74, PENTAX Optio W60, Practica, Rico and AGFAPHOTO were used to take photos. Some pictures of snowy buildings, green wall, staircase, trees, Christmas tree, pictures of sidewalk, bag, museum and car park. Some of these photos taken by mobile, orange san fransisico. The created and accessed times are in 2020 but

the modified time and EXIF tag time are between 2009 and 2012. This could mean the images were migrated from the devices to this vm in 2020.

Absent/Wrong Extension

File called ***Meunier tu Dors*** was not openable but when inspected using HEX view, the header contained markers (ftyp, isom, iso2, avc1, and mp41) which indicated it was an mp4 file and once exported and the extension was added, it was French nursery rhyme video.

2 deleted downloads, ***slacker.exe*** and ***timestop.exe*** have the wrong extension. Upon inspection using Application view, they were pictures snowy day and some plant in garden. Using HEX view, they both have **ff d8 ff e1** header which is JPEG with exif.

In **3588-Physics/Frequently Asked Questions About Light and Lasers_files** 2 JPEG files with incorrect .dll extensions found. They were images of a cake and old cell phones.

Deleted document, ***Myhiddenfile.txt*** had the wrong extension and was a JPG of a Christmas tree.

They were a few *.tmp* files that were just txt files for instance, **_WRD2478.tmp, _WRD0003.tmp**, etc.

Public/Private Keys and Digital Certificates

There was folder called ***.gnupg*** with ***private keys*** folder but it was empty. There was a private key in **../etc/ssl/private**.

In **lib/crda/pubkeys** they were 4 public keys in pem format; these are usually used to secure email and web communications.

In **../pki/fwupd**, they were GnuPG v1 and v2 public keys and in **../pki/fwupd-metadata**, they was a public key and digital certificate. The digital certificate was analyzed using **openssl** to find out who the vm was attempting to verify:

```
(base) fatima@fattiespatties2 ~ % openssl x509 -in certificate.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = LVFS CA, O = Linux Vendor Firmware Project
        Validity
            Not Before: Aug  1 00:00:00 2017 GMT
            Not After : Aug  1 00:00:00 2047 GMT
        Subject: CN = LVFS CA, O = Linux Vendor Firmware Project
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (3072 bit)
                Modulus:
                    00:b5:f5:17:1f:73:70:0c:9c:d6:ca:19:0f:c8:f7:
```

Figure 6 Analyzing Content of Digital Certificate

The organization specified by **O = Linux Vendor Firmware Project**. This is simply a secure portal that allows hardware vendors to distribute firmware updates to Linux users.

In **.cache/../mozilla/firefox/../cache2/entries** some woff files (which are used for rendering webpage fonts quickly) and some digital certificates were found. When the certificate organizations were traced similarly as above, they belonged to **Mozilla Corporation**. Check appendix for more details. This is non-suspicious activity.

Slack Files

Astronomical Names_files had 2 slack files with content: ***host.gif_slack*** and ***nineplanets32.gif-slack***. They both contained HTML that seems to be from an astronomy website associated with the Royal Observatory, Greenwich because they contained this URL: http://www.rog.nmm.ac.uk

Asteroids_files had file **Asteroid460.gif-slack** which contained a html snippet of Yahoo welcome page after a user signed up. There was link in an href to confirm email but it was using http and Yahoo had started using

HTTPS late 2012 (History of HTTPS Usage (jefftk.com)) were as this file was created on 15/03/2020. This means that this file was either from 2012 or before and then imported to the vm, or the container the file is in was created at a later date, or the file was tampered with.

951 Gaspra_files has Gaspra460.gif-slack and nine-planet32.gif-slack with hex dump, when analysed using online entropy checker Hex Analysis (online tool) | Boxentriq the entropy was close to 8 and therefore it's probably encrypted data. It couldn't be decrypted despite trying a few different methods like, John the Ripper dumps and online encryption detection.

Some of the slack files were empty and others had hex dumps but these couldn't be decrypted, since they were probably encrypted with a shared secret between the server and user and current technology can't decrypt this.

Encrypted Files

Autopsy detected 7 encrypted files: **Albert Einstein.doc**, **Hewish Word[8384].doc**, **Nicolaus Copernicus.doc, 2761-Hewish Word[8384].doc**, **4074-Nicolaus Copernicus.doc, X3fw-pwe.ncf** and **X3fw.ncf**. The last 2 encrypted files are password protected zips. They are firmware files that are encrypted by Exar to protect trade secrets. The rest of the files were .doc password protected files that were cracked using John and demonstrated in a later section.

Web Activity

The user had 11 web bookmarks, 12 cookies and some web history. There was nothing interesting here and just welcome banner, mozilla support, ubuntu wiki, etc.

Emails

2 Mails were received by rms@gnu.org on 1999-07-23 04:37:46 GST from chet@nike.ins.cwru.edu with the subject Use of Readline and had nothing suspicious.

Timeline Analysis

The vm was active from 1994 up to 2022 with most of the activity occurring in 2020 and none in 1995.

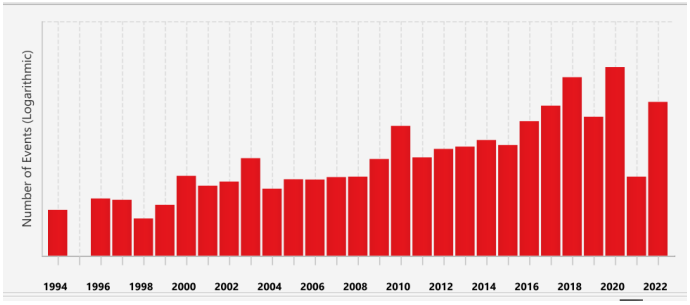
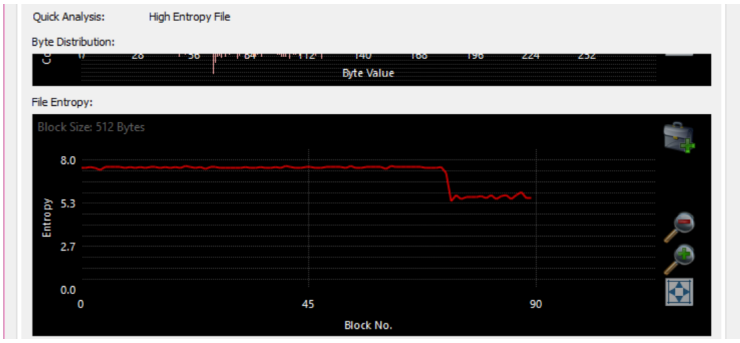


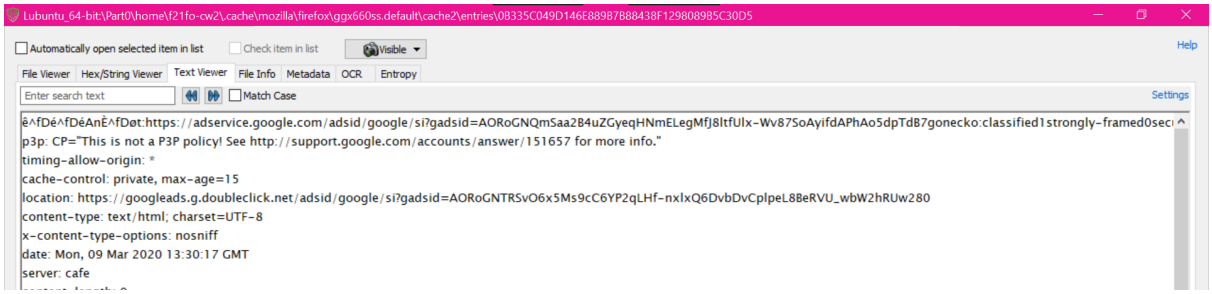
Figure 7 Timeline of Virtual Machine

3.2 Analysis using OSForensics

OS Forensics is another analysis software that has a lot of overlapping features with Autopsy such as the ability to image, file structure view and case management. It can additionally be used for live forensics, has good capabilities for analysing web traffic, email analysis and allows users to compare evidence files to known hash sets. When analysing the default Firefox profile of f21fo-cw2 user, we find a few ads, Google PNG, and some encrypted traffic. OSForensics has a built-in entropy checker, and these are the results for a file in cache, high entropy means it is probably encrypted:



OS Forensics like Autopsy also provides multiple file views like text view, hex view and file viewer. The following file was found in the Firefox default users cache, it seems to be an ad but the server is called **cafe** which is not a known server name. Similar files in this vm used **gws** server which is well known.



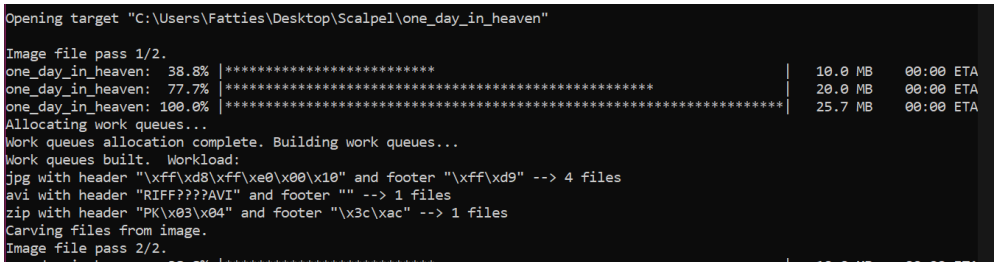
In conclusion, both tools are fairly similar but autopsy was easier to navigate since it didn't have as many pop up windows and did not have as cluttered an interface as OS Forensics. Autopsy also had a few more detailed analysis and can visualize the relationships between files in graphical form, helping understand connections between different pieces of evidence better. OS Forensics also had a few unique features such as built in entropy check and known hash file comparisons.

3.3 Additional Tools

Other files that did not show up on application view or where not part of the automatic analysis of Autopsy or OSForensics were exported from Autopsy and then analyzed using additional tools in the next sections.

3.3.1 Scalpel

Analysing ***one day in heaven*** using Scalpel:



1 avi file: rick roll video with audio.

Zip file when extracted has ***My secret.txt*** with Funkalicious.

4 image files: cat, 2 identical helicopter images (verified using MD5 hash), 1 image that could not be opened using the default image viewer: 'Photos'. When inspected using Frhed, the header and footer are correct for a jpeg file. There is also another header with an exif tag containing metadata: "An MH-60S Knighthawk helicopter flares as it lands in a cloud of dust during a training mission near Naval Air Facility El Centro, Calif., on May 25, 2005. The Knighthawk is attached to Helicopter Sea Combat Squadron 3, which trains all pilots and aircrew

reporting to MH-60S squadrons worldwide. DoD photo by Petty Officer 2nd Class Scott Taylor, U.S. Navy. (Released), NIKON CORPORATION, NIKON D1" which seems to describe the helicopter image. Once the first header is removed, the rest of the file is identical to the other helicopter files.

380 rpm files but upon inspection using **file** command in bash, rpm does not recognize these files. Since scalpel extracts files using headers, this extraction by scalpel was probably false positives.

3.3.2 Frhed

Another file that was suspected of containing embedded files (since there was a .wav header but once the complementery audio extension was added, it still wouldn't open) was **Kanbam**. When attempting to sculpt using Scalpel, Scalpel gets stuck. This could be due to false positives. When opened in Frhed, using Ctrl-F (shortcut for find) and searching common header tags, JPEG and *.wav* file headers were found. The file was then manually sculpted in Frhed and a JPG image of a person with doubled eyes and mouth was recovered and a *.wav* file of an angry cat.

3.3.3 John The Ripper – Jumbo

The encrypted files found in autopsy were cracked using john. Hashes of the files were dumped using **office2john**, a utility in John Jumbo. These dumped hashes were then cracked with John as shown:

```
seed@seed:~/john/run$ python3 office2john.py ~/Desktop/Albert\ Einstein.doc > ~/Desktop/AlbertHash.txt
seed@seed:~/john/run$ cat ~/Desktop/AlbertHash.txt
Albert Einstein.doc:$oldoffice$1*867d6947deca0b62fe61323eeccеef1d*ed7f90d4f425227d38d7e2d191877b0c*0b4acde8f1edf21481f0e4daaf1435be:
::::/home/seed/Desktop/Albert Einstein.doc
seed@seed:~/john/run$ ./john ~/Desktop/AlbertHash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (oldoffice, MS Office <= 2003 [MD5/SHA1 RC4 32/64])
Cracked 1 password hash (is in ./john.pot), use "--show"
No password hashes left to crack (see FAQ)
seed@seed:~/john/run$ ./john --show ~/Desktop/AlbertHash.txt
Albert Einstein.doc:relativity:::::/home/seed/Desktop/Albert Einstein.doc

1 password hash cracked, 0 left
```

Figure 8 Dumping Hashes of Encrypted doc and Cracking Hash

These are the recovered passwords: **Hewish Word[8384].doc** and **2761-Hewish Word[8384].doc** => wavelength; **Albert Einstein.doc** => relativity; **Nicolaus Copernicus.doc** and **4074-Nicolaus Copernicus.doc** => heliocentric. The files had information about pulsars, Albert's and Nicolaus' bibliography respectively. The 2 Hewish Work and Nicolaus Copernicus documents had the same content.

In **etc/shadow**, the hashes of the users' passwords were found and then cracked:

```
f21fo            (f21fo-cw2)
tutor123         (tutor1)
Almost done: Processing the remaining buffered candidate passwords, if any.
2g 0:00:00:29 DONE 1/3 (2024-04-04 18:33) 0.06702g/s 1627p/s 1627c/s 1627C/s Student1999991900..S999991900
Proceeding with wordlist:./password.lst
Enabling duplicate candidate password suppressor
mypassword       (student2)
```

F21fo-cw2 => **f21fo**; tutor1 => **tutor123**; student2 => **mypassword**;
Finally, after all the analysis, the image file is hashed again to verify the evidence integrity.

5 Conclusion

In conclusion, this investigation meticulously followed established forensic principles to ensure the integrity and forensic soundness of the digital evidence, the Lubuntu virtual machine. Using a variety of forensic tools, like FTK Imager and dd for evidence imaging, Autopsy and OSForensics for in-depth analysis, and specialized utilities like Scalpel and John the Ripper for file recovery and password cracking, significant amount of data was recovered. This data ranged from user activities and file manipulations to encrypted files and digital certificates, offering comprehensive insights into the usage patterns and security practices within the VM. The user seemed keen on astrology, forensics, photography, hiding files using encryption, embedding, and changing file extensions.

References

[1] Athena Forensics, “An Explanation of ACPO Guidelines for Digital Based Evidence,” *Athena Forensics*, 2018. https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics/

[2] P. Kirvan, “What is forensic image?- Definition from WhatIs.com,” WhatIs.com, Mar. 2023. https://www.techtarget.com/whatis/definition/forensic-image

[3] D. Stewart and A. Arvidsson, “Need for speed A study of the speed of forensic disk imaging tools.” Accessed: Apr. 03, 2024. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1668740/FULLTEXT02#:~:text=The%20Expert%20Witness%20Format%20is

[4] vince, “Data Dump(dd) to Create a Forensic Image with Linux – Threat Analysis.” https://vcodispot.com/data-dump-dd-create-forensic-image-linux/

Appendices

Appendix One: NIST Chain of Custody Form

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: 2 Offense: N/A

Submitting Officer: (Name/ID#) Fatima Hanif Mohammed Patel / #H00339652

Victim: N/A

Suspect: N/A

Date/Time Seized: 27 March 2024 Location of Seizure: Heriot Watt University Dubai

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
1	1	Lubuntu 64-bit.nvram
2	1	Lubuntu 64-bit.vmdk
3	1	Lubuntu 64-bit.vmsd Uncorrupted file
4	1	Lubuntu 64-bit.vmx Uncorrupted file
5	1	Lubuntu 64-bit.vmxf Uncorrupted file
6	1	Lubuntu 64-bit-s001.vmdk Uncorrupted file
7	1	Lubuntu 64-bit-s002.vmdk Uncorrupted file
8	1	Lubuntu 64-bit-s003.vmdk Uncorrupted file
9	1	Lubuntu 64-bit-s004.vmdk Uncorrupted file
10	1	Lubuntu 64-bit-s005.vmdk Uncorrupted file
11	1	Lubuntu 64-bit-s006.vmdk

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**
1 - 11	26/03/2024 3:24PM	Canvas	Desktop/Shared	Downloaded ZIP to Desktop/Shared
1-11	26/03/2024	Desktop/Shared	Desktop/Shared	Unzipped Folder to Shared
2	26/03/2024	/Shared/Evidence	FTK	Loaded evidence.
2	26/03/2024	FTK	/Shared/Evidence_Images	Created E01 and raw data images.
1-11	27/03/2024	Desktop/Shared/ Evidence	Ubuntu dd	Loading evidence into dd

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM

(Continued)

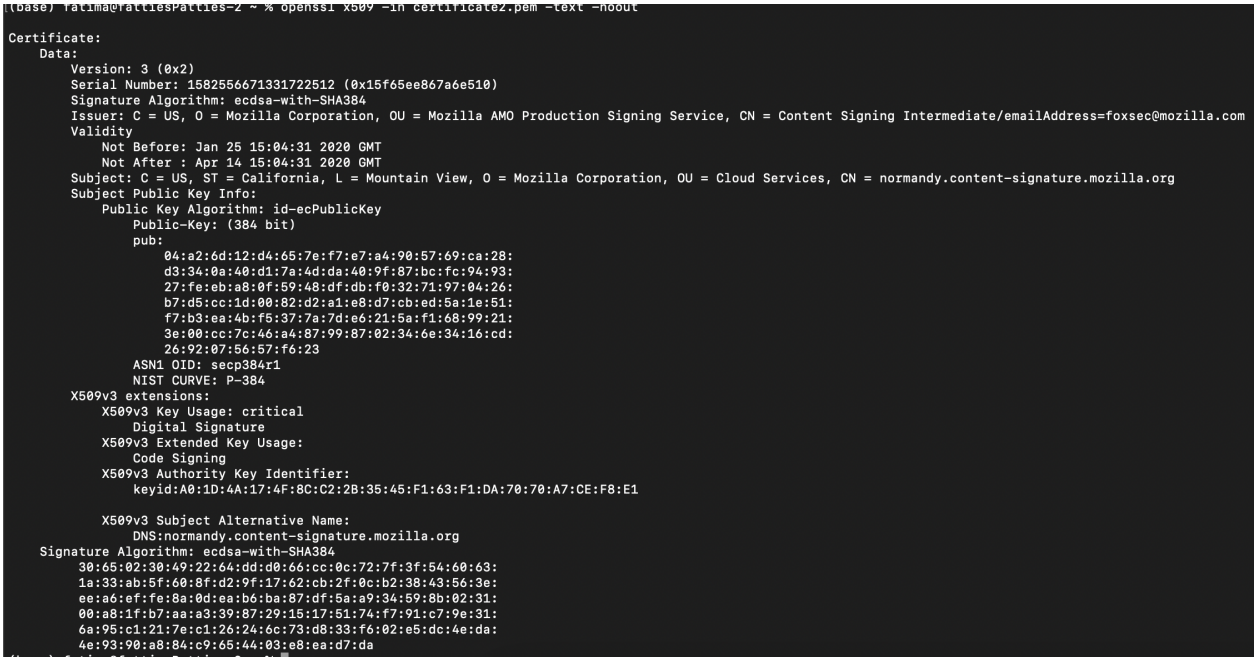
Chain of Custody				
Item #	**Date/ Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**
1-11	27/03/ 24	Ubuntu dd	Desktop/Shared/dd_ Image	Dumped image.
1-11		Desktop/Shared/d d_Image	Sha256sum	Verified integrity.
2		/Desktop/Evidence _Images	Autopsy	Loaded image and analyzedin autopsy.
2		Autopsy	Desktop/Shared	Added correct extension to ***Meunier tu Dors.***
2	28/03/ 24	Autopsy	Scalpel	Curved file One day in heaven.
2		Autopsy	Frhed	Curved file Kanbam
2	29/03/ 24	Autopsy	John the Ripper Jumbo	Cracked passwords of Albert Einstein.doc, Hewish Word[8384].doc, Nicolaus Copernicus.doc, 2761-Hewish Word[8384].doc, 4074-Nicolaus Copernicus.doc.
2		Autopsy	John the Ripper Jumbo	Cracked passwords in ../etc/shadow.
2	02/04/ 24	Desktop/Shared	OS Forensics	Analysed files.
2	02/04/ 24	Autopsy	OpenSSL	Analyzed digital Certificates.
1-11	04/04/ 24	Desktop/Shared/ dd_Image	Sha256	Verified Integirty

Appendix Two: Digital Certificates and their Contents

CERTIFICATE ONE

-----BEGIN CERTIFICATE-----
MIIC9TCCAnugAwIBAgIIFfZe6Gem5RAwCgYIKoZIzj0EAwMwgaMxCzAJBgNVBAYT
AlVTMRwwGgYDVQQKExNNb3ppbGxhIENvcnBvcmF0aW9uMS8wLQYDVQQLEyZNb3pp
bGxhIEFNTyBQcm9kdWN0aW9uIFNpZ25pbmcgU2VydmljZTFFMEMGA1UEAww8Q29u
dGVudCBTaWduaW5nIEludGVybWVkaWF0ZS9lbWFpbEFkZHJlc3M9Zm94c2VjQG1v
emlsbGEuY29tMB4XDTIwMDEyNTE1MDQzMVoXDTIwMDQxNDE1MDQzMVowgaIxCzAJ
BgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1Nb3VudGFp
biBWaWV3MRwwGgYDVQQKExNNb3ppbGxhIENvcnBvcmF0aW9uMRcwFQYDVQQLEw5D
bG91ZCBTZXJ2aWNlczEvMC0GA1UEAxMmbm9ybWFuZHkuY29udGVudC1zaWduYXR1
cmUubW96aWxsYS5vcmcwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAASibRLUZX7356SQ
V2nKKNM0CkDRek3aQJ+HvPyUkyf+66gPWUjf2/AycZcEJrfVzB0AgtKh6NfL7Voe
Ufez6kv1N3p95iFa8WiZIT4AzHxGpIeZhwI0bjQWzSaSB1ZX9iOjezB5MA4GA1Ud
DwEB/wQEAwIHgDATBgNVHSUEDDAKBggrBgEFBQcDAzAfBgNVHSMEGDAWgBSgHUoX
T4zCKzVF8WPx2nBwp8744TAxBgNVHREEKjAogiZub3JtYW5keS5jb250ZW50LXNp
Z25hdHVyZS5tb3ppbGxhLm9yZzAKBggqhkjOPQQDAwNoADBlAjBJImTd0GbMDHJ/
P1RgYxozq19gj9KfF2LLLwyyOENWPu6m7/6KDeq2uoffWqk0WYsCMQCoH7eqozmH
KRUXUXT3kceeMWqVwSF+wSYkbHPYM/YC5dxO2k6TkKiEyWVEA+jq19o=
-----END CERTIFICATE-----

CERTIFICATE ONE CONTENT



```
(base) fatima@fattiesPatties-2 ~ % openssl x509 -in certificate2.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1582556671331722512 (0x15f65ee867a6e510)
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = US, O = Mozilla Corporation, OU = Mozilla AMO Production Signing Service, CN = Content Signing Intermediate/emailAddress=foxsec@mozilla.com
        Validity
            Not Before: Jan 25 15:04:31 2020 GMT
            Not After : Apr 14 15:04:31 2020 GMT
        Subject: C = US, ST = California, L = Mountain View, O = Mozilla Corporation, OU = Cloud Services, CN = normandy.content-signature.mozilla.org
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:a2:6d:12:d4:65:7e:f7:e7:a4:90:57:69:ca:28:
                    d3:34:0a:40:d1:7a:4d:da:40:9f:87:bc:fc:94:93:
                    27:fe:eb:a8:0f:59:48:df:db:f0:32:71:97:04:26:
                    b7:d5:cc:1d:00:82:d2:a1:e8:d7:cb:ed:5a:1e:51:
                    f7:b3:ea:4b:f5:37:7a:7d:e6:21:5a:f1:68:99:21:
                    3e:00:cc:7c:46:a4:87:99:87:02:34:6e:34:16:cd:
                    26:92:07:56:57:f6:23
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                Code Signing
            X509v3 Authority Key Identifier:
                keyid:A0:1D:4A:17:4F:8C:C2:2B:35:45:F1:63:F1:DA:70:70:A7:CE:F8:E1

            X509v3 Subject Alternative Name:
                DNS:normandy.content-signature.mozilla.org
    Signature Algorithm: ecdsa-with-SHA384
         30:65:02:30:49:22:64:dd:d0:66:cc:0c:72:7f:3f:54:60:63:
         1a:33:ab:5f:60:8f:d2:9f:17:62:cb:2f:0c:b2:38:43:56:3e:
         ee:a6:ef:fe:8a:0d:ea:b6:ba:87:df:5a:a9:34:59:8b:02:31:
         00:a8:1f:b7:aa:a3:39:87:29:15:17:51:74:f7:91:c7:9e:31:
         6a:95:c1:21:7e:c1:26:24:6c:73:d8:33:f6:02:e5:dc:4e:da:
         4e:93:90:a8:84:c9:65:44:03:e8:ea:d7:da
```

CERTIFICATE TWO

-----BEGIN CERTIFICATE-----
MIIFezCCA2OgAwIBAgIDEAAEMA0GCSqGSIb3DQEBDAUAMH0xCzAJBgNVBAYTAlVT
MRwwGgYDVQQKExNNb3ppbGxhIENvcnBvcmF0aW9uMS8wLQYDVQQLEyZNb3ppbGxh
IEFNTyBQcm9kdWN0aW9uIFNpZ25pbmcgU2VydmljZTEfMB0GA1UEAxMWcm9vdC1j
YS1wcm9kdWN0aW9uLWFtbzAeFw0xOTAyMDEyMjA2NDVaFw0yMTAxMzEyMjA2NDVa
MIGjMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTTW96aWxsYSBDb3Jwb3JhdGlvbjEv
MC0GA1UECxMmTW96aWxsYSBBTU8gUHJvZHVjdGlvbiBTaWduaW5nIFNlcnZpY2Ux
RTBDBgNVBAMMPENvbnRlbnQgU2lnbmluZyBJbnRlcm1lZGlhdGUvZW1haWxBZGRy
ZXNzPWZveHNlY0Btb3ppbGxhLmNvbTB2MBAGByqGSM49AgEGBSuBBAAiA2IABCSV
pyWrz0Eo9xgh9R1VLgkX+lnGNNU6VhV2PhAnnGikcCeBeRSCBiSQePS2ZlURytes

JWrWoS0H+TvBdeRTgc32tftZxSSSwKUMmZRDappvM/uLbSrd6kY2rntETaneEqOC
AYkwggGFMAwGA1UdEwQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMBYGA1UdJQEB/wQM
MAoGCCsGAQUFBwMDMB0GA1UdDgQWBBSgHUoXT4zCKzVF8WPx2nBwp8744TCBqAYD
VR0jBIGgMIGdgBSzvOpYdKvhbngqsqucIx6oYyyXt6GBgaR/MH0xCzAJBgNVBAYT
AlVTMRwwGgYDVQQKExNNb3ppbGxhIENvcnBvcmF0aW9uMS8wLQYDVQQLEyZNb3pp
bGxhIEFNTyBQcm9kdWN0aW9uIFNpZ25pbmcgU2VydmljZTEfMB0GA1UEAxMWcm9v
dC1jYS1wcm9kdWN0aW9uLWFtb4IBATAzBglghkgBhvhCAQQEJhYkaHR0cDovL2Fk
ZG9ucy5hbGxpem9tLm9yZy9jYS9jcmwucGVtME4GA1UdHgRHMEWgQzAggh4uY29u
dGVudC1zaWduYXR1cmUubW96aWxsYS5vcmcwH4IdY29udGVudC1zaWduYXR1cmUu
bW96aWxsYS5vcmcwDQYJKoZIhvcNAQEMBQADggIBAG519ZvKmtUWL6+3CaU1n6L+
y0EIueOH+PjZX6ZToj6baPtQgWSCGKsEjZtpystkvLh2DCEdQllBjuUEQ11atPaG
96Xp4l7VbaOUYEfoZxi3kpMLEOXUGvdcNFkj4KZY6rhYNhXV9lCkj1JCV+6iUpps
8yIE5vykGtQPRSWIH/bqvLD4U1Qy7gzxqBK2pV+YkzrA7d2bfwDpnz8gZYhb7e7p
EUvT7W+vJlrhrGLMTQ0A1jMEc+daiePr6/r/pSbXgHIdwUCgbRH2MPWje1ciXrHp
Xw6cJz8lw73564AMBI3FaCV1iqouuMF54Tfk3zyyfGQs6+xEhQBbaHHGN+NdwE+U
3yfiTtgHwblxv/B7bVtvoGGfXd2SrTZtPxsdD8MwllNaAsdMhFDhkJ9Mufhxb6QF
+nxG9Qxn0+eJayoUHwe8XIXAW89s8uibv+zMiidrq9Dr5VJkhXZ6mvQTC9RPu/UE
at2t/z+FKIZOSBwpjIvr0hJbUhZJewKfW9ivCwhTstjcit9ZaTW/7Iml+zS657P0
fhygYvD/FczJD80MjMsrV3a+2H+oyL8yFuSMr1NO3G0e1BY4OKaLknto4ch6Qiqg
e45q0ccPgC24r5RhShwXRMK88Vt0f/d8+KH8OBztqBuhzAzrZXL2BHFuChf1e1Ql
tHN7fk4u+dLUHYv0ulzu
-----END CERTIFICATE-----

CERTIFICATE TWO CONTENT

```
(base) fatima@fattiesPatties-2 ~ % openssl x509 -in certificate3.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1048580 (0x100004)
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: C = US, O = Mozilla Corporation, OU = Mozilla AMO Production Signing Service, CN = root-ca-production-amo
        Validity
            Not Before: Feb  1 22:06:45 2019 GMT
            Not After : Jan 31 22:06:45 2021 GMT
        Subject: C = US, O = Mozilla Corporation, OU = Mozilla AMO Production Signing Service, CN = Content Signing Intermediate/emailAddress=foxsec@mozilla.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:24:95:a7:25:ab:cf:41:28:f7:18:21:f5:1d:55:
                    2e:09:17:fa:59:c6:34:d5:3a:56:15:76:3e:10:27:
                    9c:68:a4:70:27:81:79:14:82:06:24:90:78:f4:b6:
                    66:55:11:ca:d7:ac:25:6a:d6:a1:2d:07:f9:3b:c1:
                    75:e4:53:81:cd:f6:b5:fb:59:c5:24:92:c0:a5:0c:
                    99:94:43:6a:9a:6f:33:fb:8b:6d:2a:dd:ea:46:36:
                    ae:7b:44:4d:a9:de:12
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Extended Key Usage: critical
                Code Signing
            X509v3 Subject Key Identifier:
                A0:1D:4A:17:4F:8C:C2:2B:35:45:F1:63:F1:DA:70:70:A7:CE:F8:E1
            X509v3 Authority Key Identifier:
                keyid:B3:BC:EA:58:74:AB:E1:6E:78:2A:B2:AB:9C:23:1E:A8:63:2C:97:B7
                DirName:/C=US/O=Mozilla Corporation/OU=Mozilla AMO Production Signing Service/CN=root-ca-production-amo
                serial:01

            Netscape CA Revocation Url:
                http://addons.allizom.org/ca/crl.pem
            X509v3 Name Constraints:
                Permitted:
                  DNS:.content-signature.mozilla.org
                  DNS:content-signature.mozilla.org

    Signature Algorithm: sha384WithRSAEncryption
         6e:75:f5:9b:ca:9a:d5:16:2f:af:b7:09:a5:35:9f:a2:fe:cb:
         41:08:b9:e3:87:f8:f8:d9:5f:a6:53:a2:3e:9b:68:fb:50:81:
         64:82:18:ab:04:8d:9b:69:ca:cb:64:bc:b8:76:0c:21:1d:40:
         89:41:8e:e5:04:43:5d:5a:b4:f6:86:f7:a5:e9:e2:5e:d5:6d:
         a3:94:60:47:e8:67:18:b7:92:93:0b:10:e5:d4:1a:f7:5c:34:
         59:23:e0:a6:58:ea:b8:58:36:15:d5:f6:50:a4:8f:52:42:57:
         ee:a2:52:9a:6c:f3:22:04:e6:fc:a4:1a:d4:0f:45:25:88:1f:
         f6:ea:bc:b0:f8:53:54:32:ee:0c:f1:a8:12:b6:a5:5f:98:93:
         3a:c0:ed:dd:9b:7f:00:e9:9f:3f:20:65:88:5b:ed:ee:e9:11:
         4b:d3:ed:6f:af:26:5a:e1:ac:62:cc:4d:0d:00:d6:33:04:73:
         e7:5a:89:e3:eb:eb:fa:ff:a5:26:d7:80:72:1d:c1:40:a0:6d:
         11:f6:30:f5:a3:7b:57:22:5e:b1:e9:5f:0e:9c:27:3f:08:c3:
         bd:f9:eb:80:0c:04:8d:c5:68:25:75:8a:aa:2e:b8:c1:79:e1:
         37:e4:df:3c:b2:7c:64:2c:eb:ec:44:85:00:5b:68:71:c6:37:
         e3:5d:c0:4f:94:df:27:e2:4e:d8:07:c1:b9:71:bf:f0:7b:6d:
         5b:6f:a0:61:9f:5d:dd:92:ad:36:6d:3f:1b:1d:0f:c3:30:96:
         53:5a:02:c7:4c:84:50:e1:90:9f:4c:b9:f8:71:6f:a4:05:fa:
         7c:46:f5:0c:67:d3:e7:89:6b:2a:14:1f:07:bc:5c:85:c0:5b:
         cf:6c:f2:e8:9b:bf:ec:cc:8a:27:6b:ab:d0:eb:e5:52:64:85:
         76:7a:9a:f4:13:0b:d4:4f:bb:f5:04:6a:dd:ad:ff:3f:85:28:
         86:4e:48:1c:29:8c:8b:eb:d2:12:5b:52:16:49:7b:02:9f:5b:
         d8:af:0b:08:53:b2:d8:dc:8a:df:59:69:35:bf:ec:89:a5:fb:
         34:ba:e7:b3:f4:7e:1c:a0:62:f0:ff:15:cc:c9:0f:cd:0c:8c:
```

CERTIFICATE THREE

-----BEGIN CERTIFICATE-----
MIIGYTCCBEmgAwIBAgIBATANBgkqhkiG9w0BAQwFADB9MQswCQYDVQQGEwJVUzEc
MBoGA1UEChMTTW96aWxsYSBDb3Jwb3JhdGlvbjEvMC0GA1UECxMmTW96aWxsYSBB
TU8gUHJvZHVjdGlvbiBTaWduaW5nIFNlcnZpY2UxHzAdBgNVBAMTFnJvb3QtY2Et
cHJvZHVjdGlvbi1hbW8wHhcNMTUwMzE3MjI1MzU3WhcNMjUwMzE0MjI1MzU3WjB9
MQswCQYDVQQGEwJVUzEcMBoGA1UEChMTTW96aWxsYSBDb3Jwb3JhdGlvbjEvMC0G
A1UECxMmTW96aWxsYSBBTU8gUHJvZHVjdGlvbiBTaWduaW5nIFNlcnZpY2UxHzAd
BgNVBAMTFnJvb3QtY2EtcHJvZHVjdGlvbi1hbW8wggIgMA0GCSqGSIb3DQEBAQUA
A4ICDQAwggIIAoICAQC0u2HXXbrwy36+MPeKf5jgoASMfMNz7mJWBecJgvlTf4hH
JbLzMPsIUauzI9GEpLfHdZ6wzSyFOb4AM+D1mxAWhuZJ3MDAJOf3B1Rs6QorHrl8
qqlNtPGqepnpNJcLo7JsSqqE3NUm72MgqIHRgTRsqUs+7LIPGe7262U+N/T0LPYV
Le4rZ2RDHoaZhYY7a9+49mHOI/g2YFB+9yZjE+XdplT2kBgA4P8db7i7I0tIi4b0
B0N6y9MhL+CRZJyxdFe2wBykJX14LsheKsM1azHjZO56SKNrW8VAJTLkpRxCmsiT
r08fnPyDKmaeZ0BtsugicdipcZpXriIGmsZbI12q5yuwjSELdkDV6Uajo2n+2ws5
uXrP342X71WiWhC/dF5dz1LKtjBdmUkxaQMOP/uhtXEKBrZo1ounDRQx1j7+SkQ4
BEwjB3SEtr7XDWGOcOIkoJZWPACfBLC3PJCBWjTAyBlud0C5n3Cy9regAAnOIqI1
t16GU2laRh7elJ7gPRNgQgwLXeZcFxw6wvyiEcmCjOEQ6PM8UQjthOsKlszMhlKw
vjyOGDoztkqSBy/v+Asx7OW2Q7rlVfKarL0mREZdSMfoy3zTgtMVCM0vhNl6zcvf
5HNNopoEdg5yuXo2chZ1p1J+q86b0G5yJRMeT2+iOVY2EQ37tHrqUURncCy4uwIB
A6OB7TCB6jAMBgNVHRMEBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAWBgNVHSUBAf8E
DDAKBggrBgEFBQcDAzCBkgYDVR0jBIGKMIGHoYGBpH8wfTELMAkGA1UEBhMCVVMx
HDAaBgNVBAoTE01vemlsbGEgQ29ycG9yYXRpb24xLzAtBgNVBAsTJk1vemlsbGEg
QU1PIFByb2R1Y3Rpb24gU2lnbmluZyBTZXJ2aWNlMR8wHQYDVQQDExZyb290LWNh
LXByb2R1Y3Rpb24tYW1vggEBMB0GA1UdDgQWBBSzvOpYdKvhbngqsqucIx6oYyyX
tzANBgkqhkiG9w0BAQwFAAOCAgEAaNSRYAaECAePQFyfk12kl8UPLh8hBNidP2H6
KT6O0vCVBjxmMrwr8Aqz6NL+TgdPmGRPDDLPDpDJTdWzdj7khAjxqWYhutACTew5
eWEaAzyErbKQl+duKvtThhV2p6F6YHJ2vutu4KIciOMKB8dslIqIQr90IX2Usljq
8Ttdyf+GhUmazqLtoB0GOuESEqT4unX6X7vSGu1oLV20t7t5eCnMMYD67ZBn0YIU
/cm/+pan66hHrja+NeDGF8wabJxdqKItCS3p3GN1zUGuJKrLykxqbOp/21byAGog
Z1amhz6NHUcfE6jki7sM7LHjPostU5ZWs3PEfVVgha9fZUhOrIDsyXEpCWVa3481
LlAq3GiUMKZ5DVRh9/Nvm4NwrTfB3QkQQJCwfXvO9pwnPKtISYkZUqhEqvXk5nBg
QCkDSLDjXTx39naBBGIVIqBtKKuVTla9enngdq692xX/CgO6QJVrwpqdGjebj5P8
5fNZPABzTezG3Uls5Vp+4iIWVAEDkK23cUj3c/HhE+Oo7kxfUeu5Y1ZV3qr61+6t
ZARKjbu1TuYQHf0fs+GwID8zeLc2zJL7UzcHFwwQ6Nda9OJN4uPAuC/BKaIpxCLL
26b24/tRam4SJjqpiq20lynhUrmTtt6hbG3E1Hpy3bmkt2DYnuMFwEx2gfXNcnbT
wNuvFqc=
-----END CERTIFICATE-----

CERTIFICATE THREE CONTENT

```
(base) fatima@fattiesPatties-2 ~ % openssl x509 -in certificate4.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: C = US, O = Mozilla Corporation, OU = Mozilla AMO Production Signing Service, CN = root-ca-production-amo
        Validity
            Not Before: Mar 17 22:53:57 2015 GMT
            Not After : Mar 14 22:53:57 2025 GMT
        Subject: C = US, O = Mozilla Corporation, OU = Mozilla AMO Production Signing Service, CN = root-ca-production-amo
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:b4:bb:61:d7:5d:ba:f0:cb:7e:be:30:f7:8a:7f:
                    98:e0:a0:04:8c:7c:c3:73:ee:62:56:05:e7:09:82:
                    f9:53:7f:88:47:25:b2:f3:30:fb:08:51:ab:b3:23:
                    d1:84:a4:b7:c7:75:9e:b0:cd:2c:85:39:be:00:33:
                    e0:f5:9b:10:16:86:e6:49:dc:c0:c0:24:e7:f7:07:
                    54:6c:e9:0a:2b:1e:b9:7c:aa:a9:4d:b4:f1:aa:7a:
                    99:e9:34:97:0b:a3:b2:6c:4a:aa:84:dc:d5:26:ef:
                    63:20:a8:81:d1:81:34:6c:a9:4b:3e:ec:b2:0f:19:
                    ee:f6:eb:65:3e:37:f4:f4:2c:f6:15:2d:ee:2b:67:
                    64:43:1e:86:99:85:86:3b:6b:df:b8:f6:61:ce:23:
                    f8:36:60:50:7e:f7:26:63:13:e5:dd:a6:54:f6:90:
                    18:00:e0:ff:1d:6f:b8:bb:23:4b:48:8b:86:f4:07:
                    43:7a:cb:d3:21:2f:e0:91:64:9c:b1:74:57:b6:c0:
                    1c:a4:25:7d:78:2e:c8:5e:2a:c3:35:6b:31:e3:64:
                    ee:7a:48:a3:6b:5b:c5:40:25:32:e4:a5:1c:42:9a:
                    c8:93:af:4f:1f:9c:fc:83:2a:66:9e:67:40:6d:b2:
                    e8:22:71:d8:a9:71:9a:57:ae:22:06:9a:c6:5b:23:
                    5d:aa:e7:2b:b0:8d:21:0b:76:40:d5:e9:46:a3:a3:
                    69:fe:db:0b:39:b9:7a:cf:df:8d:97:ef:55:a2:5a:
                    10:bf:74:5e:5d:cf:52:ca:b6:30:5d:99:49:31:69:
                    03:0e:3f:fb:a1:b5:71:0a:06:b6:68:d6:8b:a7:0d:
                    14:31:d6:3e:fe:4a:44:38:04:4c:23:07:74:84:b6:
                    be:d7:0d:61:8e:70:e2:24:a0:96:56:3c:00:9f:04:
                    b0:b7:3c:90:81:5a:34:c0:c8:19:6e:77:40:b9:9f:
                    70:b2:f6:b7:a0:00:09:ce:22:a2:35:b7:5e:86:53:
                    69:5a:46:1e:de:94:9e:e0:3d:13:60:42:0c:0b:5d:
                    e6:5c:17:1c:3a:c2:fc:a2:11:c9:82:8c:e1:10:e8:
                    f3:3c:51:08:ed:84:eb:0a:96:cc:cc:86:52:b0:be:
                    3c:8e:18:3a:33:b6:4a:92:07:2f:ef:f8:0b:31:ec:
                    e5:b6:43:ba:e5:55:f2:9a:ac:bd:26:44:46:5d:48:
                    c7:e8:cb:7c:d3:82:d3:15:08:cd:2f:84:d9:7a:cd:
                    cb:df:e4:73:4d:a2:9a:04:76:0e:72:b9:7a:36:72:
                    16:75:a7:52:7e:ab:ce:9b:d0:6e:72:25:13:1e:4f:
                    6f:a2:39:56:36:11:0d:fb:b4:7a:ea:51:44:67:70:
                    2c:b8:bb
                Exponent: 3 (0x3)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Extended Key Usage: critical
                Code Signing
            X509v3 Authority Key Identifier:
                DirName:/C=US/O=Mozilla Corporation/OU=Mozilla AMO Production Signing Service/CN=root-ca-production-amo
                serial:01

            X509v3 Subject Key Identifier:
                B3:BC:EA:58:74:AB:E1:6E:78:2A:B2:AB:9C:23:1E:A8:63:2C:97:B7
    Signature Algorithm: sha384WithRSAEncryption
         68:d4:91:60:06:84:08:07:8f:40:5c:9f:93:5d:a4:97:c5:0f:
         2e:1f:21:04:d8:9d:3f:61:fa:29:3e:8e:d2:f0:95:06:3c:66:
         32:bc:2b:f0:0a:b3:e8:d2:fe:4e:07:4f:98:64:4f:0c:32:cf:
         0e:90:c9:4d:d5:b3:76:3e:e4:84:08:f1:a9:66:21:ba:d0:02:
```

PRIVATE KEY

-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDH5pm/aF3/Nw0F
Z6+wSq362dTCxR7xI2xyunMP9ROHD1vpg+HV9t0/T9FvSZZAdoR5J4aLewn4gGIZ
WhNoOvXtSf4c/dn6BNUDIfbQNeDfss6sbWiUDl8gMbb2R0vBAHTHREK9HVJ79zHn
CywJGSeAKGMjVfczAaoAHHC+7fADRbHceJUF7h+iu0E0AKw0QkU4MkFSav5Hdvv+
Tj1fCUborqF44MKYsiw+YV5j63WX97fBWG1WmbYhm7QopL6+a6u1mpeSbhj3E+ON
xLhU8Ga9vfjdTE9EhrLIF1HzM4s6rYJVHqsuM79BaY8MhrgH5FDSP8nCPw0pitwO
7OErp/lnAgMBAAECggEAVdhBzmETfLY3cUrFt/9aF4/UPpBIaWW8/Mf1AbVNXYLL
Bc0M/sW03at5VUFUtPowiZbfwKZl8cGwXxK/otMvKWfNKMYbBbNthprfUyrQF0DC
YGnbrzk8wKaY28piTc/UVn6J6ozdDz9ovr+deYrD29V8PYB9V/ou9z0/bb7gg4Z4
PnSge1MS8Gat5c7uJl9d4CLTbZPvnstK6HfVPUNI/mq1axESKQ0i1IhOxShCBMsw
tRnxy2il1XZTrHhKHPyvjuZEcfz7i74NkPEIfPCSyFrNrC3fM8x4N5AGXsEeedvG
80pL1TAwAzI+GWbs2pPqTmNcPhMnuuoRXtZtHUgBAQKBgQDjqGSKyNOtj6yimT4w
p9j/ngFy4dUZSMkzrCxAz+TPLXEQNE2GPMeDL3ZMxASd1tApXKoX1Kb8IiwkUGPC
Pe9lwq4ormXAoi/7ZGZ3XwWXz4SRZTbQ2G2sEGJIz7PWV/V5G40B9PhykM7WYZPE
csdEgj5vXFqNxA6twkF1mtmnyQKBgQDgyZLQBjQTcZGeWGxvISxAzdmY4N+P1Koz
jC1b/DfEaf8+HRNVceYvqkAtl0BIbVm3bqBMugfRckyyBUL2xyeaHA6/4UEggvAx
YD+a68rwLWjLY7/QfXTAPawH/Ef9sy40dTpYvwQ9O20oCxp7EGBjLWN+ems2WrLv
yHNs132PrwKBgH+PDe7Zggng0/kzZi47DhKEBQnK0e1d5CbI1O7nzavsKUrME5gg
nCW8RUvUFUYfY/mZC1FY/MuPli4uwQbIT0g0YgM3XJooBjyUz/kYy/h49S3GiYVR
j3n2oCtt/bUfCdL3BfZPvZnr24kxmWtcaJzRYYxiMfb3IMZpbuYngsdJAoGBANTu
/WyjQ7dbcIaf2m/W67Wjicmg0wXLfUMBOYKWRDmB8zBimIrrLxLd4peNXG5/b2os
mBq2amuEK5TDGTDtbN02UN6AwZHLlz4en4HgdMfZLBjmr7AO94aXpRuXZpazokQ8
+/1PTPO4FGnHQtlqpPOt7j7ENkUx26j6qCRlaOKvAoGAV9pTqtR/QAVIJcSt4aZ3
vZcELuZH3q9HhgACUrm9fGx4vXDN74/m57Tg40qVImvUHK3n7RIPK690sOw+z97o
9t/zvWcKWzBP9x13W7O8SGrrz7W3WShiJliaTHSbyitNf37bJTeikiUEW4anDafl
H6o7NasSCfSZZIvhmVw2IKQ=
-----END PRIVATE KEY-----

Screenshot of OS Forensics