Informe Preliminar

1. Introducción al caso

Se ha iniciado una investigación en materia de **Informática Forense**, con el objetivo de determinar si los equipos de cómputo dentro de la empresa han sido utilizados con fines distintos a los laborales, es decir; si dichos equipos se han usado para extraer información confidencial, si hay o hubo comunicación a correos electrónicos no autorizados (cuentas personales, cuentas de la competencia, etc.), si intencionalmente algún usuario eliminó información, si algún equipo se utiliza para realizar actividades de "hacking", entre otras más.

Para dicha investigación se contrataron los servicios del perito en Informática Forense, Aarón Chávez, quien está acreditado en la materia y como experto deberá realizar el análisis informático para determinar si hay usuarios que estén haciendo mal uso de los activos de información de la empresa.

2. Resumen general

Durante el presente proceso de investigación en cómputo forense **se han desarrollado hasta este momento las siguientes actividades:**

I. Se designó al Primer Respondiente.
II. Se han identificado plenamente los dispositivos de dónde se ha obtenido evidencia digital.
III. Se han registrado los dispositivos en la Cadena de Custodia.
IV. Se ha elaborado un inventario de los dispositivos que son fuente de evidencia digital.
V. Se han realizado adquisiciones estáticas y adquisiciones en vivo, con el objetivo de preservar la evidencia digital.
VI. Se han creado Imágenes Forenses de Contenido Personalizado.

Hasta este punto las actividades que se han desarrollado, han permitido identificar las fuentes de evidencia digital, preservar la evidencia usando técnicas de informática forense y realizar un análisis preliminar a partir de dicha evidencia.

3. Inventario de evidencia identificada

A continuación se hace la relación específica de la evidencia que se ha preservado y sobre la que se está realizando el análisis:

Evidencia	Fuente	Criterio de selección	Herramienta usada para su adquisición
EV001	Dispositivo externo USB	Memoria USB dónde se comparte información internamente.	**EWF Acquire** (Paladin)
EV002	Dispositivo externo USB	Memoria USB dónde se comparte información internamente.	**dc3dd**
EV003	Disco duro externo con una partición NTFS.	En este dispositivo se copia información en equipos con Windows.	**FTK-Imager**
EV004	Computadora utilizada por la asistente del Gerente.	Debido a que es un equipo por donde fluye bastante información de la empresa.	**EWF Acquire** (Paladin)
EV005	Computadora Linux utilizada por el encargado de sistemas.	Es otro de los equipos importantes a analizar, ya que se trata del equipo utilizado por el encargado de los Sistemas Informáticos en la empresa.	**EWF Acquire** (Paladin)

Se decidieron utilizar estas herramientas para la adquisición de las imágenes forenses por la razón de que permiten manejar formatos estándares, además de que ofrecen la posibilidad de crear bloques, niveles de compresión, verificación y cálculo de la integridad de las mismas.

4. Reportes de adquisición de evidencia

Como se mencionó en el punto anterior (punto No. 3), una de las razones por la que se decidieron usar las herramientas de adquisición forense mencionadas en el punto anterior, es porque permiten garantizar su integridad.

A continuación se presenta la información técnica que determina que la información obtenida es íntegra respecto a las fuentes de donde se obtuvieron.

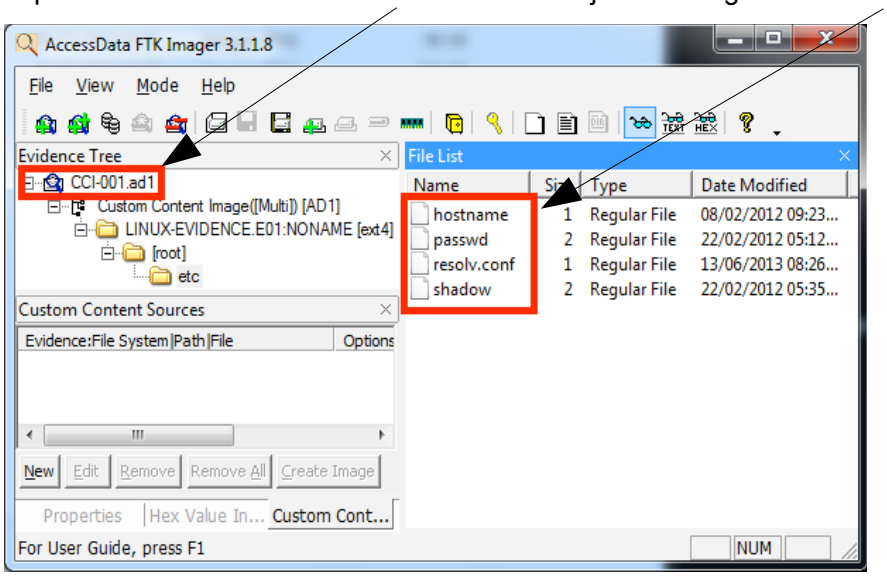
Evidencia	HASH de la fuente de evidencia	HASH de la imagen forense	Observaciones
EV001	**MD5:** 7157c30699544b203833219e4c039fae	**MD5:** 7157c30699544b203833219e4c039fae	Coinciden ambos HASH.
	SHA1: 9f4e5c264f100e6cc6335ad529defacе1bb40b59	**SHA1:** 9f4e5c264f100e6cc6335ad529defacе1bb40b59	Coinciden ambos HASH.
EV002	**MD5 Bloque 1 (EV002.000):** 564d8db9a77ea51ea6b09ec731dd7059	**MD5 Bloque 1 (EV002.000):** 564d8db9a77ea51ea6b09ec731dd7059	Coinciden ambos HASH.
	MD5 Bloque 2 (EV002.001): 4eefc6fe38f0c53f76d90c7f3e9990a0	**MD5 Bloque 2 (EV002.001):** 4eefc6fe38f0c53f76d90c7f3e9990a0	Coinciden ambos HASH.
	MD5 Bloque 3 (EV002.002): 391ed2830172742537dacda3c2e7c992	**MD5 Bloque 3 (EV002.002):** 391ed2830172742537dacda3c2e7c992	Coinciden ambos HASH.
	MD5 Bloque 4 (EV002.003): 2013e0cb38ccf97b0fbc688a25c54403	**MD5 Bloque 4 (EV002.003):** 2013e0cb38ccf97b0fbc688a25c54403	Coinciden ambos HASH.
	MD5 Bloque 5 (EV002.004): 962e9a21fe1fef7e0c6041090018ce5f	**MD5 Bloque 5 (EV002.004):** 962e9a21fe1fef7e0c6041090018ce5f	Coinciden ambos HASH.
	MD5 Bloque 6 (EV002.005): 6bf2910ff74c66447630496cc9881f83	**MD5 Bloque 6 (EV002.005):** 6bf2910ff74c66447630496cc9881f83	Coinciden ambos HASH.
	MD5 Bloque 7 (EV002.006): 984e192c2a97886fd124a1e1be5094e4	**MD5 Bloque 7 (EV002.006):** 984e192c2a97886fd124a1e1be5094e4	Coinciden ambos HASH.
	MD5 Bloque 8 (EV002.007): 9293950d73d9812e4af48e80c256c2e4	**MD5 Bloque 8 (EV002.007):** 9293950d73d9812e4af48e80c256c2e4	Coinciden ambos HASH.
	MD5 Bloque 9 (EV002.008): cca6655688ce269bfa50c21a4f5f8367	**MD5 Bloque 9 (EV002.008):** cca6655688ce269bfa50c21a4f5f8367	Coinciden ambos HASH.
EV003	**MD5:** 2c4abc7ac52651ee75e64da95f252da0	**MD5:** 2c4abc7ac52651ee75e64da95f252da0	Coinciden ambos HASH.
	SHA1: bbe1e7649dd7f726b57053d7904214e165b8d567	**SHA1:** bbe1e7649dd7f726b57053d7904214e165b8d567	Coinciden ambos HASH.
EV004	**MD5:** 5f23f3e377deec20b85b6b3789365aba	**MD5:** 5f23f3e377deec20b85b6b3789365aba	Coinciden ambos HASH.
	SHA1: 2bea618af4a9bfb530b269050ef26a743cb816f8	**SHA1:** 2bea618af4a9bfb530b269050ef26a743cb816f8	Coinciden ambos HASH.
EV005	**MD5:** 4d6402dbd5842423677dc761b5d9	**MD5:** 4d6402dbd5842423677dc761b5d9	Coinciden ambos HASH.

	31fd **SHA1:** 2459c0c590d40a10e465088eb85e1a731aaa227a	31fd **SHA1:** 2459c0c590d40a10e465088eb85e1a731aaa227a	Coinciden ambos HASH.

5. Información general de los sistemas preservados

Durante el análisis de los dispositivos que se identificaron se encontraron los siguientes usuarios en los sistemas operativos de dichos equipos:

Equipo con Linux:
A partir de la imagen personalizada llamada **CCI-001.ad1** se extrajeron los siguientes archivos:

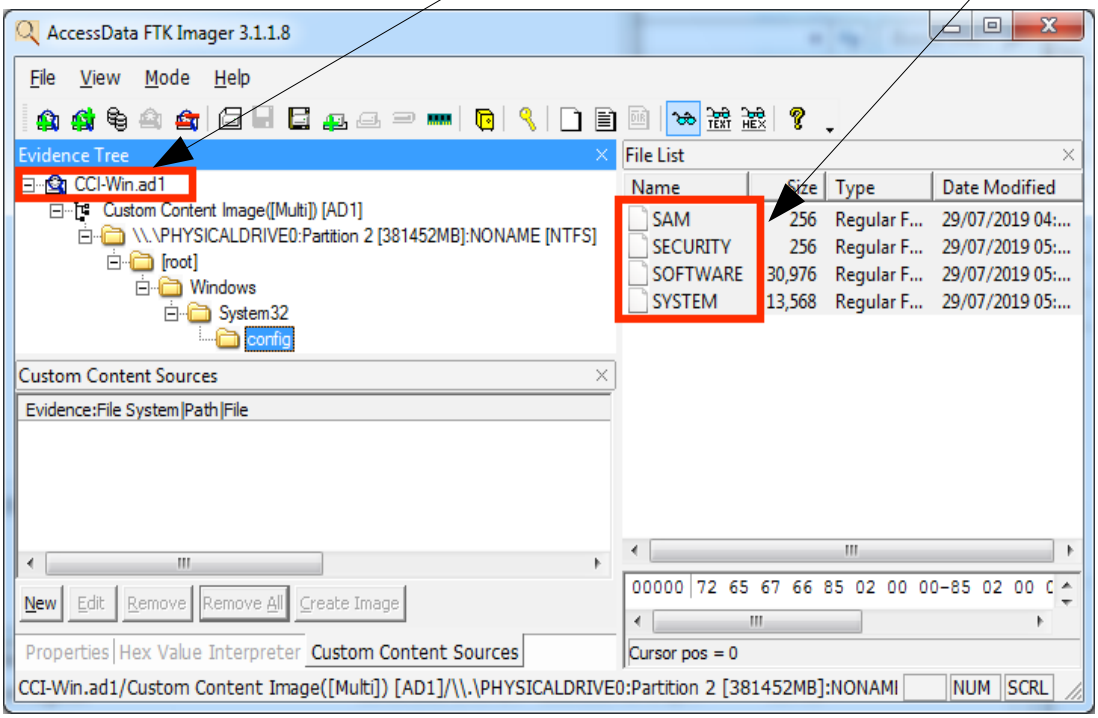


A continuación se muestra el contenido del archivo **passwd**, el cual está en formato de texto plano y contiene la **lista de los nombres de los usuarios** en el equipo de cómputo con **Linux**:

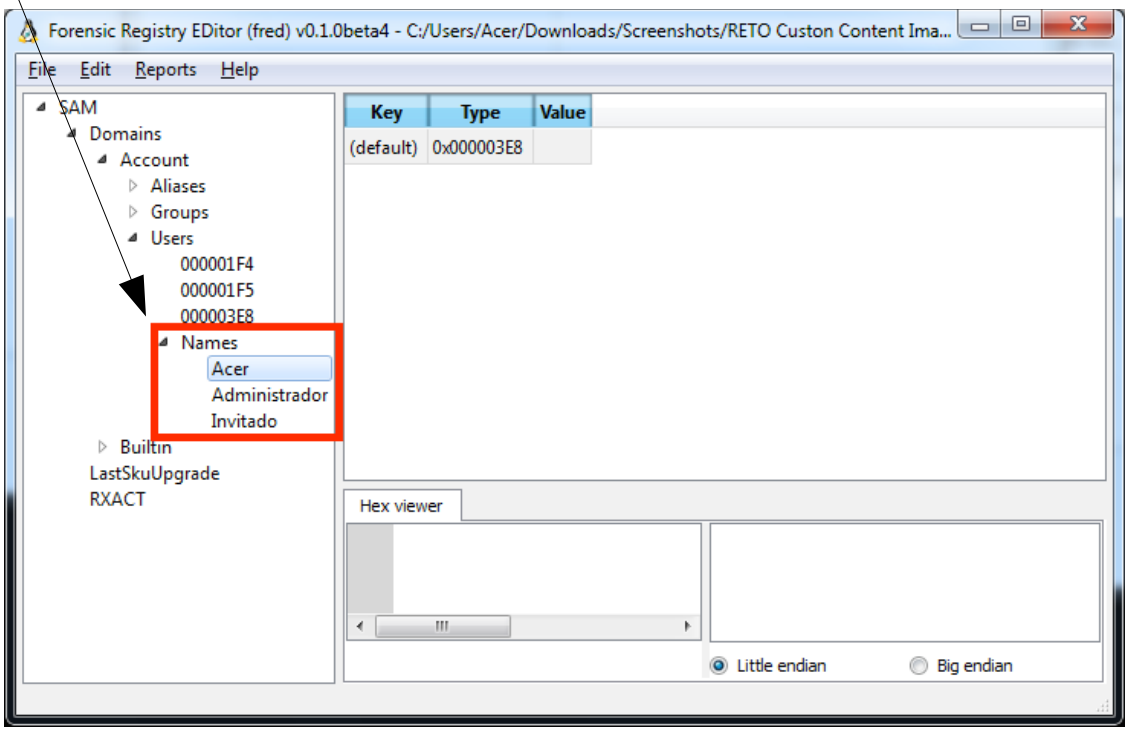
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:107::/var/run/dbus:/bin/false
avahi-autoipd:x:103:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:104:111:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
couchdb:x:105:113:CouchDB Administrator,,,:/var/lib/couchdb:/bin/bash
speech-dispatcher:x:106:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
usbmux:x:107:46:usbmux daemon,,,:/home/usbmux:/bin/false
haldaemon:x:108:114:Hardware abstraction layer,,,:/var/run/hald:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:110:115:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:117:RealtimeKit,,,:/proc:/bin/false
saned:x:112:118::/home/saned:/bin/false

hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
gdm:x:114:120:Gnome Display Manager:/var/lib/gdm:/bin/false
aaron:x:1000:1000:Aaron Chavez,,,:/home/aaron:/bin/bash
usuario:x:1001:1001:usuario,,,,:/home/usuario:/bin/bash
mysql:x:115:123:MySQL Server,,,:/var/lib/mysql:/bin/false
postgres:x:116:124:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash

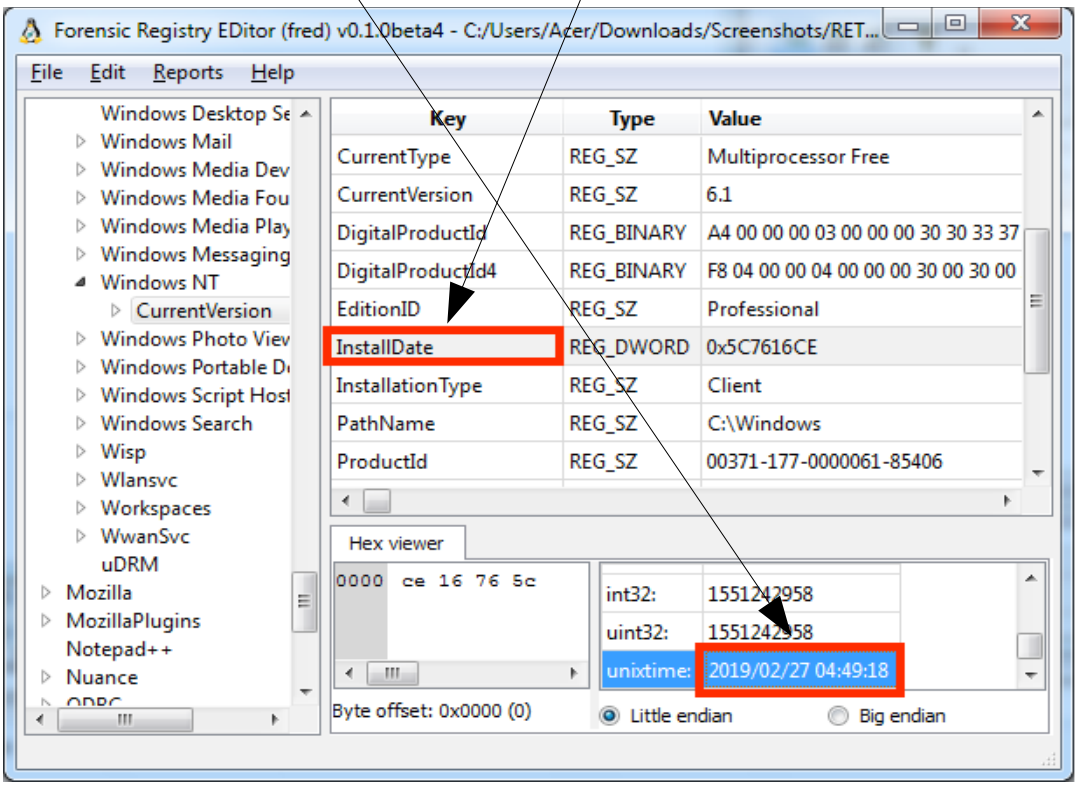
Equipo con Windows:
A partir de la imagen personalizada llamada **CCI-Win.ad1** se extrajeron los siguientes archivos:



Después se analizó el archivo **SAM** con la herramienta **FRED** (Forensic Registry Editor) para obtener la **lista de los nombres de usuario** en el equipo de cómputo con **Windows**:

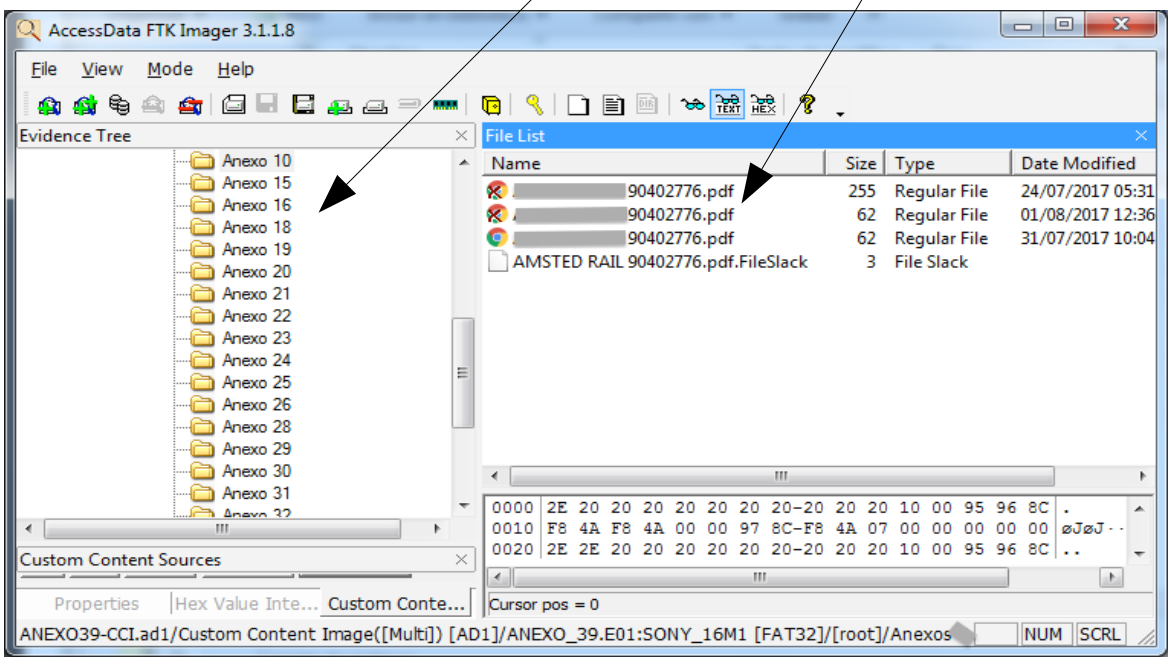


También haciendo un análisis del archivo **SOFTWARE** mediante la herramienta FRED, se obtuvo un dato importante como lo es la **fecha y hora en que se instaló por primera vez el Sistema Operativo Windows**:



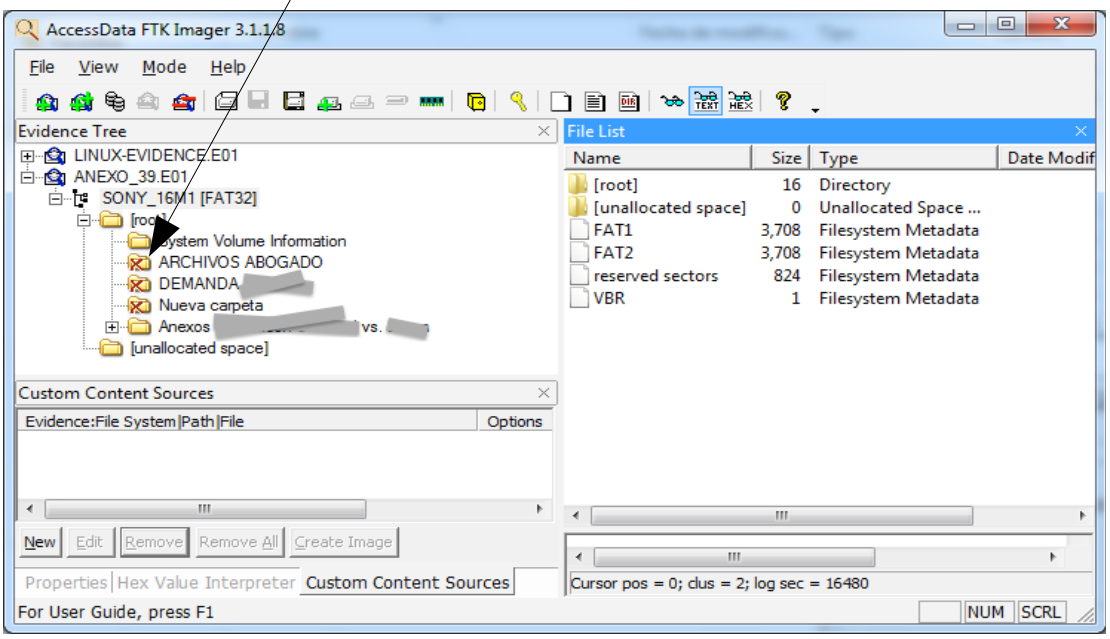
6. Información encontrada en las imágenes forenses

La información que se ha encontrado en las imágenes forenses adquiridas y que hasta el momento falta analizarlas a profundidad, es información como **carpetas de usuario y documentos diversos**, como se ilustra a continuación:



7. Hallazgos preliminares, si existen

En una de las imágenes forenses adquiridas **se encontró un hallazgo importante** y es que **algunas carpetas parecen haber sido eliminadas**, como se ilustra a continuación:



8. Siguientes pasos

Los pasos a seguir para concluir esta investigación serán:

- Realizar un **análisis de la demás información** contenida en las imágenes forenses.
- Análisis de los ***logs* del sistema**.
- Realizar un análisis de los **procesos ejecutados**.
- Presentación de los resultados mediante un **informe técnico** y un **informe ejecutivo**.
- **Presentación ante la autoridad** que solicitó esta investigación.