PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

Ing. Francesco SACCIA

WWW.STUDIOSACCIA.IT

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

PROVE DIGITALI:

- Files (doc, txt, exl, pdf, jpg, bmp, etc.)
- Files audio e video
- File di log
- Email, PEC
- Social Network (Facebook, Twitter)
- Instant messaging (WhatsApp, WeChat, etc)
- Chiamate, sms
- Pagine Web
- Contratti stipulati online
- Copie digitalizzate

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

STRUMENTI INFORMATICI:

- Supporti Informatici:
  1. Notebook, PC, Hard Disk esterni, Pen USB, etc.
  2. Smartphone e tablet
- Internet (WEB)
  1. Facebook, Youtube, Twitter, Forum, etc.

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

PRODUZIONE PROVE DIGITALI:

- Precedente Processo Penale
- Nuova acquisizione delle Parti in causa nel p.c.

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

NORMATIVA di RIFERIMENTO:

- Standard ISO 27037 - è uno standard internazionale contenente linee guida per l'identificazione, la raccolta, l'acquisizione, la conservazione e il trasporto di evidenze digitali

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

PROCEDURA ACQUISIZIONE FORENSE – I FASE

VERIFICA CATENA CUSTODIA

- Memorie di massa
- Notebook, Pc, Server, Nas
- Smartphone e Tablet

ANALISI DATI IDENTIFICATIVI

- Marca, modello
- Serial Number
- n° HD interni
- IMEI - SIMCARD

STUDIO SACCIA

PROCEDURA ACQUISIZIONE FORENSE – II FASE

STRUMENTI DI ACQUISIZIONE

- Duplicatori HW (Ditto, Tableau, Falcon, UFED)
- Software (Axiom, Encase, etc.)
- Comando DD sistemi operativi Linux

COPIA FORENSE

- File o più files nel formato prescelto (DD, RAW, IMG, E01, etc.)
- File di report dell'operazione di acquisizione svolta

REPORT ACQUISIZIONE Hard Disk:

Physical Image E01:

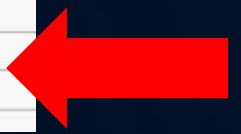
Target File Name:	HDD_HITACHI_SN_X0GNSUMR		
Image File Segment Size:	2147483648	**Compression Type:**	Empty Block
Source HPA/DCO:	Indicate Only	**EWF File Format:**	encase6
Buffer Size:	1M	**Read Error Retries:**	
Error Granularity:			
Swap Byte Pairs of the Media Data:	Disabled	**Wipe Sectors on Read Error:**	Disabled

eSATA Extended Disk Info [Show]

USB-DA1 Extended Disk Info [Show]

Log [Hide]

Timestamp (CET)	Type	User	Message
Dec 04, 2017 10:15:24	Physical Image	panel	Starting Physical Image E01 action from eSATA to USB-DA1, partition 1.
Dec 04, 2017 12:26:33	Physical Image	panel	Finished Physical Image E01 action.
Dec 04, 2017 12:26:33	Physical Image	panel	md5 hash value: 7478B5CE3C1E82A89DA4BCCD25B992A5
Dec 04, 2017 12:26:33	Physical Image	panel	sha1 hash value: 81416D1C1792F7FBCC074AE2649BFC2475359A8E



STUDIO SACCIA

FUNZIONE DI HASH:

L'hash è una funzione matematica univoca ed unidirezionale. Applicando una funzione di hash a un file o ad un intero hard disk, si ottiene una sequenza alfanumerica, che rappresenta una sorta di "*impronta digitale*" dei dati, e viene detta valore di hash

Gli algoritmi di hash, in particolare SHA1 e MD5, sono utilizzati per validare e in qualche modo "*firmare*" digitalmente i dati acquisiti. La recente legislazione impone infatti una catena di custodia che permetta di preservare i reperti informatici da eventuali modifiche successive all'acquisizione: tramite i codici hash è possibile in ogni momento verificare che quanto repertato sia rimasto immutato nel tempo

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

PROCEDURA ACQUISIZIONE FORENSE – III FASE

RICERCA E CATALOGAZIONE

- Software (Axiom, Encase, FTK, Ufed, etc.)
- Ricerca manuale

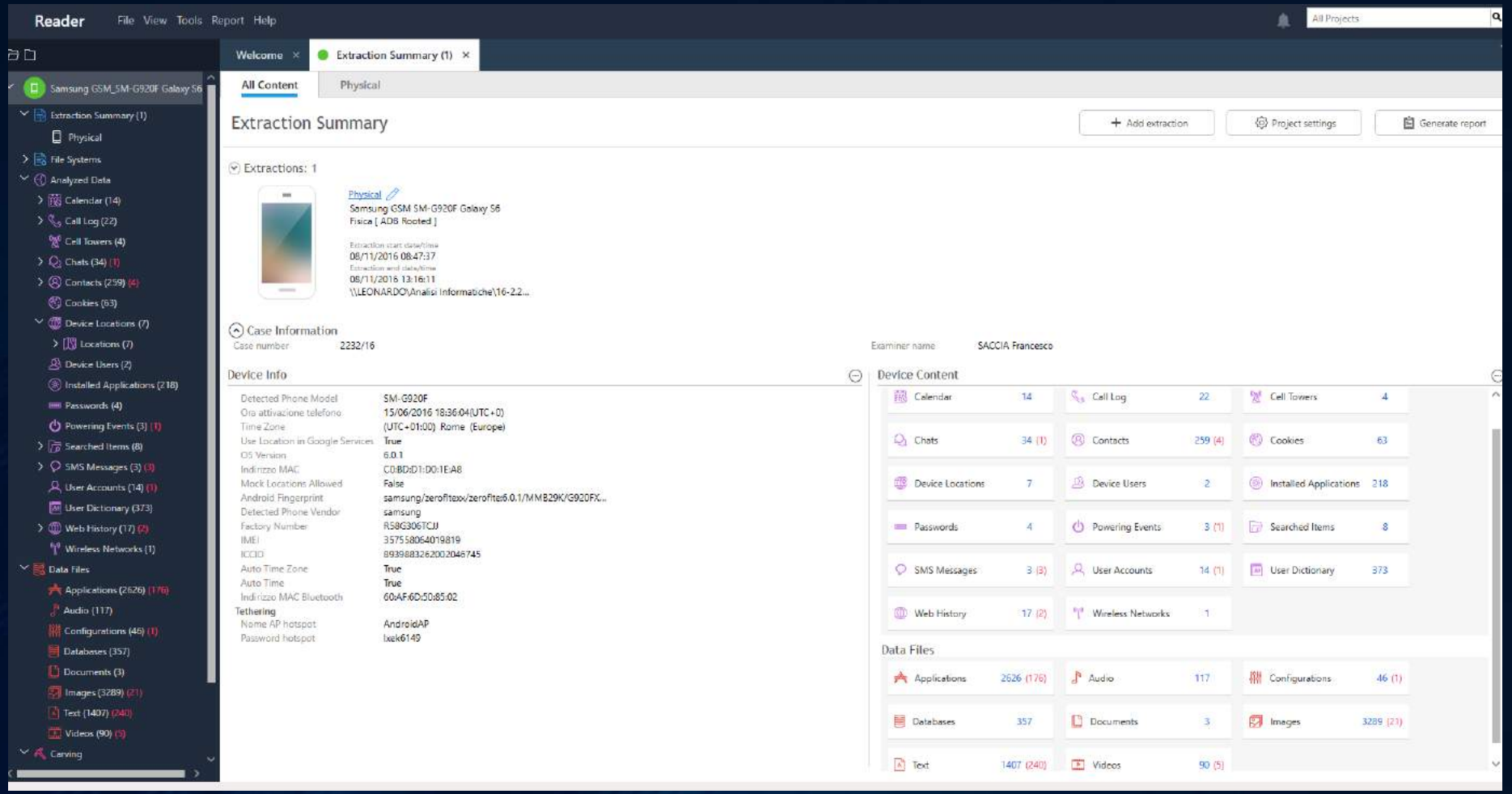
REPORT

- File di report completo o parziale
- Estrapolazione files
- Estrapolazione di informazioni

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI SMARTPHONE – UFED:



STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI SMARTPHONE – UFED:

Device Info

Detected Phone Model	SM-G920F
Ora attivazione telefono	15/06/2016 18:36:04(UTC+0)
Time Zone	(UTC+01:00) Rome (Europe)
Use Location in Google Services	True
OS Version	6.0.1
Indirizzo MAC	C0:BD:D1:D0:1E:A8
Mock Locations Allowed	False
Android Fingerprint	samsung/zerofltexx/zeroflte:6.0.1/MMB29K/G920FX...
Detected Phone Vendor	samsung
Factory Number	R58G306TCJJ
IMEI	357558064019819
ICCID	8939883262002046745
Auto Time Zone	True
Auto Time	True
Indirizzo MAC Bluetooth	60:AF:6D:50:85:02
Tethering	
Nome AP hotspot	AndroidAP
Password hotspot	lxek6149

Device Content

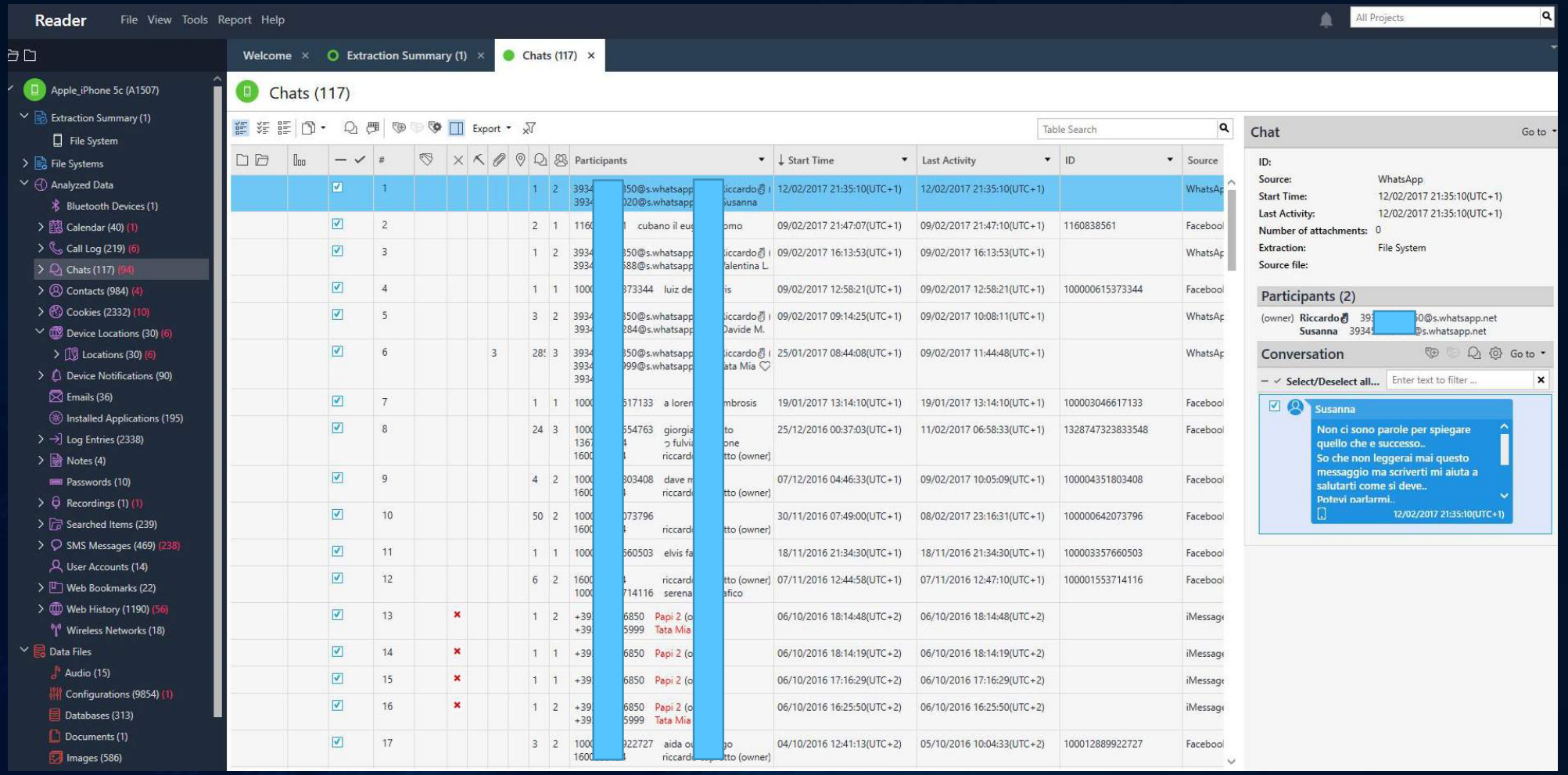
Phone Data

Calendar	14	Call Log	22	Cell Towers	4
Chats	34 (1)	Contacts	259 (4)	Cookies	63
Device Locations	7	Device Users	2	Installed Applications	218
Passwords	4	Powering Events	3 (1)	Searched Items	8
SMS Messages	3 (3)	User Accounts	14 (1)	User Dictionary	373
Web History	17 (2)	Wireless Networks	1		

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI SMARTPHONE – UFED:



STUDIO SACCIA

Crittografia end-to-end (chat WhatsApp)

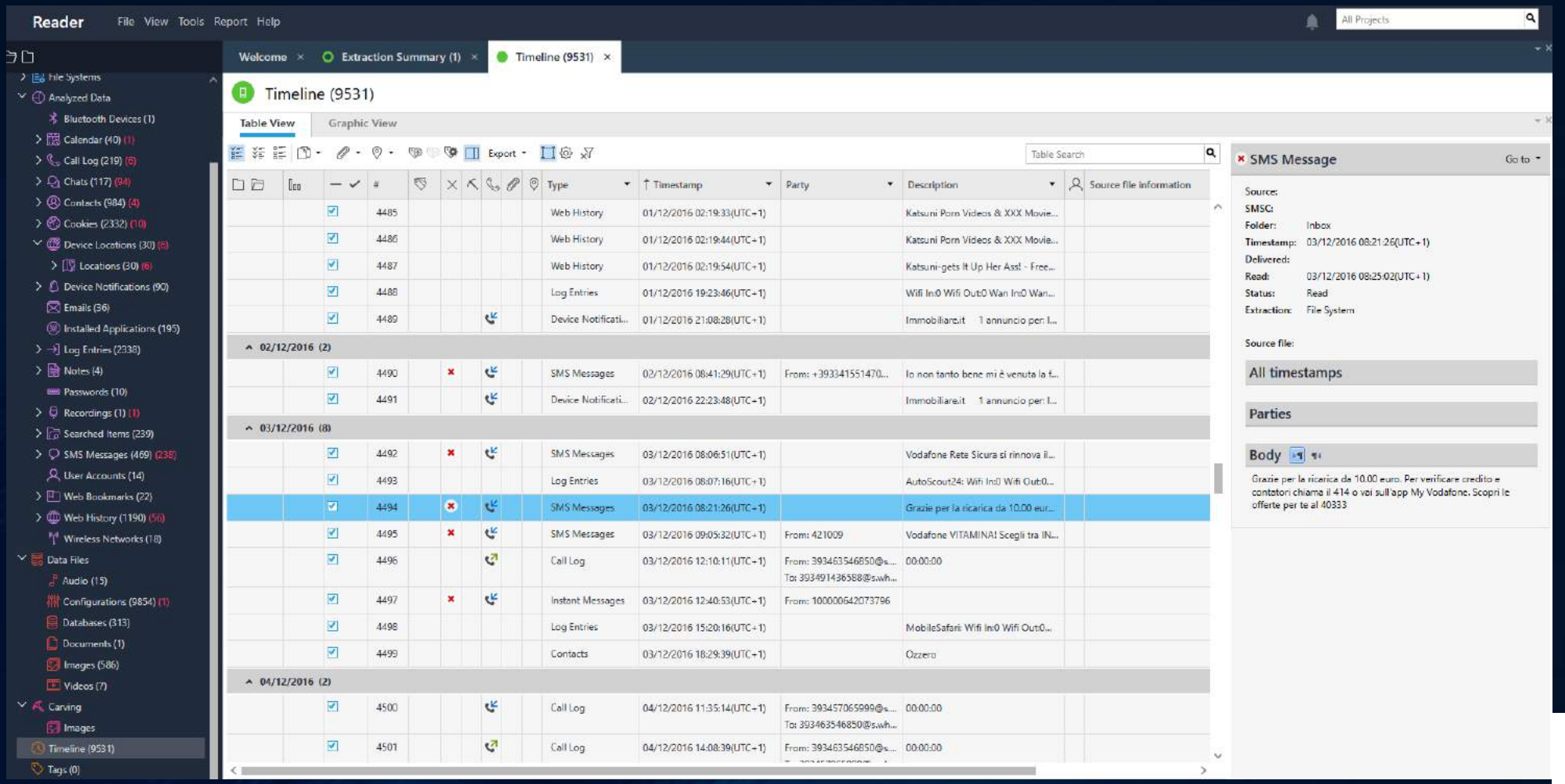
LA CRITTOGRAFIA END-TO-END DI WHATSAPP ASSICURA CHE SOLO TU E LA PERSONA CON CUI STAI COMUNICANDO POSSIATE LEGGERE CIÒ CHE VIENE INVIATO, E NESSUN ALTRO, NEMMENO WHATSAPP. I MESSAGGI SONO PROTETTI CON DEI LUCCHETTI, E SOLO TU E IL TUO DESTINATARIO AVETE LE CHIAVI SPECIALI NECESSARIE PER SBLOCCARLE E LEGGERLE I MESSAGGI. PER UNA MAGGIORE PROTEZIONE, OGNI MESSAGGIO INVIATO HA UN PROPRIO LUCCHETTO E UNA PROPRIA CHIAVE UNICI.

NESSUNA AUTORITÀ POTRÀ MAI CHIEDERE A WHATSAPP I CONTENUTI DELLE CHIAMATE E DEI MESSAGGI, POICHÉ LA STESSA WHATSAPP NON HA LA POSSIBILITÀ DI PRENDERNE VISIONE

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

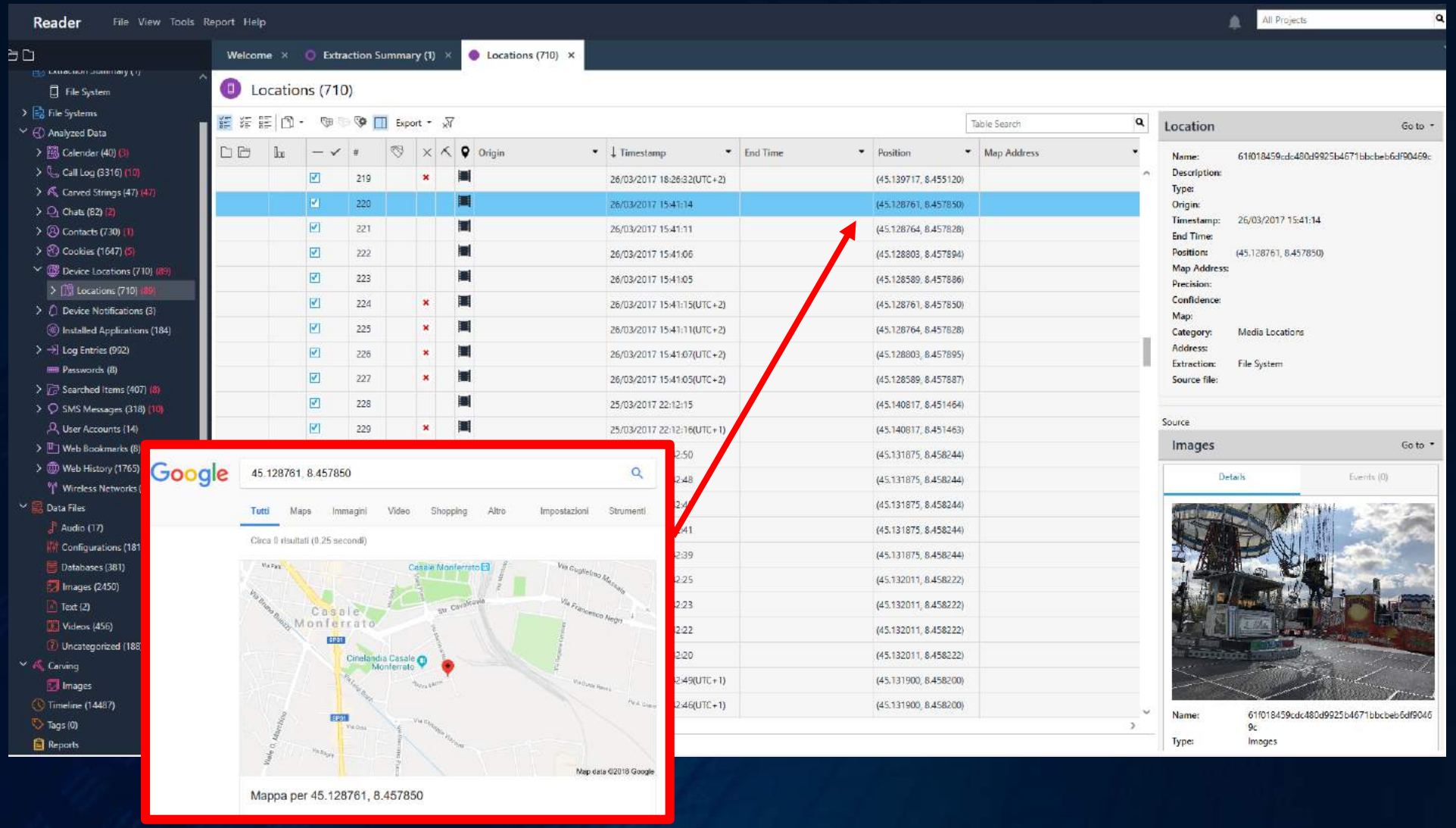
ANALISI SMARTPHONE – UFED:



STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

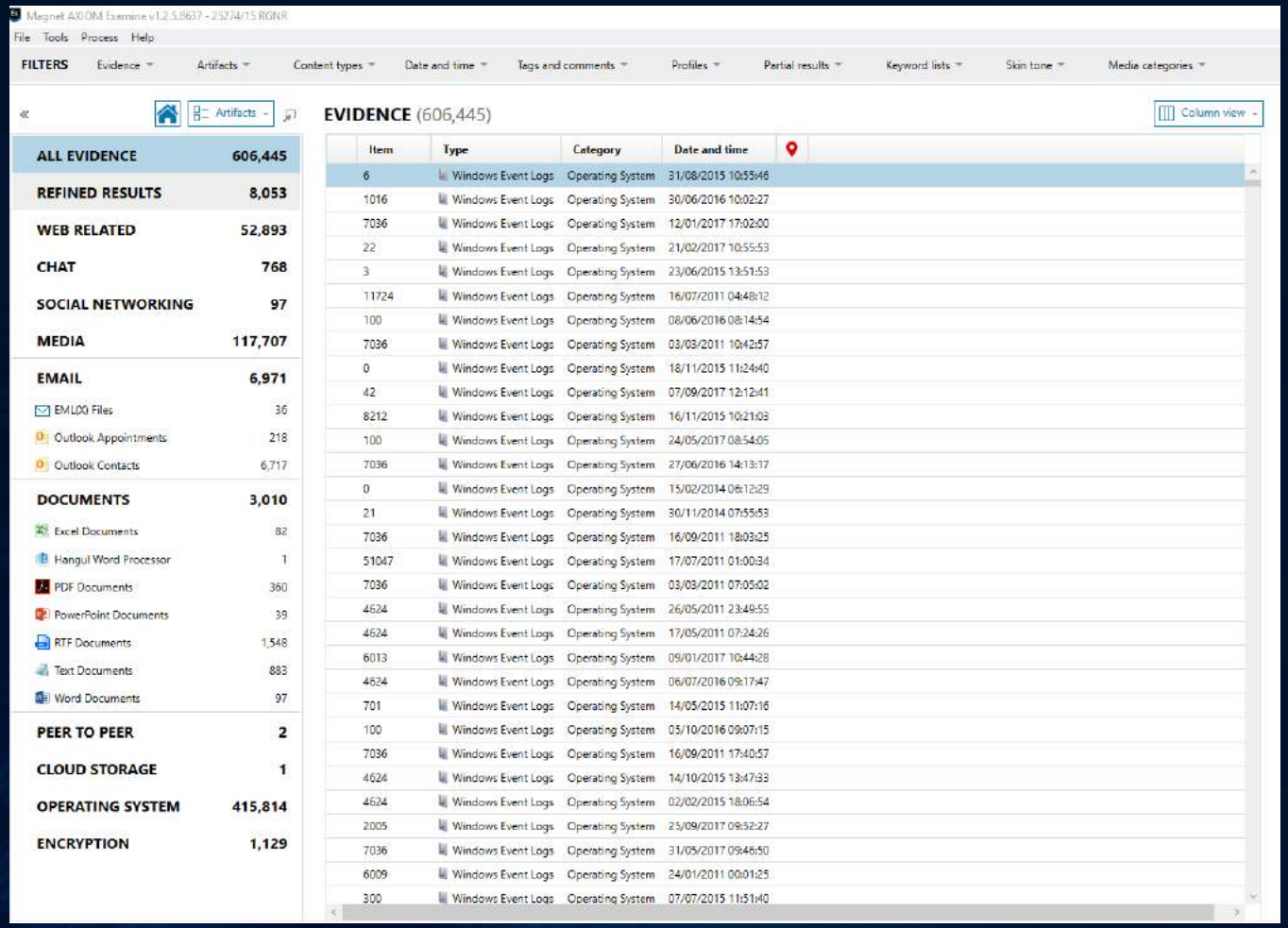
ANALISI SMARTPHONE – UFED:



STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

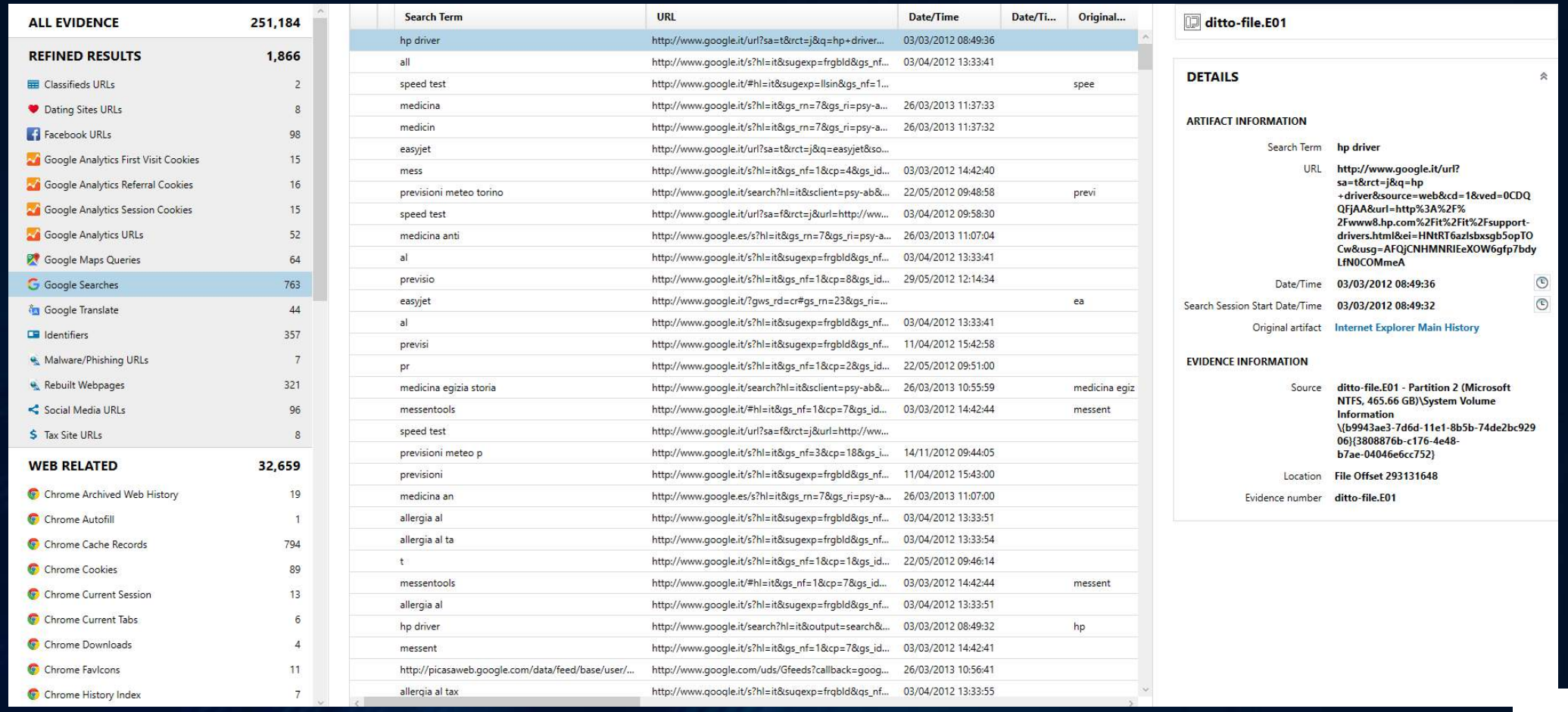
ANALISI Hard Disk – AXIOM:



STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI Hard Disk – AXIOM:



ALL EVIDENCE	**251,184**
REFINED RESULTS	**1,866**
Classifieds URLs	2
Dating Sites URLs	8
Facebook URLs	98
Google Analytics First Visit Cookies	15
Google Analytics Referral Cookies	16
Google Analytics Session Cookies	15
Google Analytics URLs	52
Google Maps Queries	64
Google Searches	763
Google Translate	44
Identifiers	357
Malware/Phishing URLs	7
Rebuilt Webpages	321
Social Media URLs	96
Tax Site URLs	8
WEB RELATED	**32,659**
Chrome Archived Web History	19
Chrome Autofill	1
Chrome Cache Records	794
Chrome Cookies	89
Chrome Current Session	13
Chrome Current Tabs	6
Chrome Downloads	4
Chrome Favicons	11
Chrome History Index	7

Search Term	URL	Date/Time	Date/Ti...	Original...
hp driver	http://www.google.it/url?sa=t&rct=j&q=hp+driver...	03/03/2012 08:49:36		
all	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	03/04/2012 13:33:41		
speed test	http://www.google.it/#hl=it&sugexp=llsin&gs_nf=1...			spee
medicina	http://www.google.it/s?hl=it&gs_rn=7&gs_ri=psy-a...	26/03/2013 11:37:33		
medicin	http://www.google.it/s?hl=it&gs_rn=7&gs_ri=psy-a...	26/03/2013 11:37:32		
easyjet	http://www.google.it/url?sa=t&rct=j&q=easyjet&so...			
mess	http://www.google.it/s?hl=it&gs_nf=1&cp=4&gs_id...	03/03/2012 14:42:40		
previsioni meteo torino	http://www.google.it/search?hl=it&sclient=psy-ab&...	22/05/2012 09:48:58		previ
speed test	http://www.google.it/url?sa=f&rct=j&url=http://ww...	03/04/2012 09:58:30		
medicina anti	http://www.google.es/s?hl=it&gs_rn=7&gs_ri=psy-a...	26/03/2013 11:07:04		
al	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	03/04/2012 13:33:41		
previsio	http://www.google.it/s?hl=it&gs_nf=1&cp=8&gs_id...	29/05/2012 12:14:34		
easyjet	http://www.google.it/?gws_rd=cr#gs_rn=23&gs_ri=...			ea
al	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	03/04/2012 13:33:41		
previsi	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	11/04/2012 15:42:58		
pr	http://www.google.it/s?hl=it&gs_nf=1&cp=2&gs_id...	22/05/2012 09:51:00		
medicina egizia storia	http://www.google.it/search?hl=it&sclient=psy-ab&...	26/03/2013 10:55:59		medicina egiz
messentools	http://www.google.it/#hl=it&gs_nf=1&cp=7&gs_id...	03/03/2012 14:42:44		messent
speed test	http://www.google.it/url?sa=f&rct=j&url=http://ww...			
previsioni meteo p	http://www.google.it/s?hl=it&gs_nf=3&cp=18&gs_i...	14/11/2012 09:44:05		
previsioni	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	11/04/2012 15:43:00		
medicina an	http://www.google.es/s?hl=it&gs_rn=7&gs_ri=psy-a...	26/03/2013 11:07:00		
allergia al	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	03/04/2012 13:33:51		
allergia al ta	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	03/04/2012 13:33:54		
t	http://www.google.it/s?hl=it&gs_nf=1&cp=1&gs_id...	22/05/2012 09:46:14		
messentools	http://www.google.it/#hl=it&gs_nf=1&cp=7&gs_id...	03/03/2012 14:42:44		messent
allergia al	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	03/04/2012 13:33:51		
hp driver	http://www.google.it/search?hl=it&output=search&...	03/03/2012 08:49:32		hp
messent	http://www.google.it/s?hl=it&gs_nf=1&cp=7&gs_id...	03/03/2012 14:42:41		
http://picasaweb.google.com/data/feed/base/user/...	http://www.google.com/uds/Gfeeds?callback=goog...	26/03/2013 10:56:41		
allergia al tax	http://www.google.it/s?hl=it&sugexp=frgbld&gs_nf...	03/04/2012 13:33:55		

ditto-file.E01

DETAILS

ARTIFACT INFORMATION

Search Term	**hp driver**
URL	**http://www.google.it/url?sa=t&rct=j&q=hp+driver&source=web&cd=1&ved=0CDQQFjAA&url=http%3A%2F%2Fwww8.hp.com%2Fit%2Fit%2Fsupport-drivers.html&ei=HNtRT6azlsbxsgb5opTOCw&usg=AFQjCNHMNRIEeXOW6gfp7bdyLfN0COMmeA**
Date/Time	**03/03/2012 08:49:36**
Search Session Start Date/Time	**03/03/2012 08:49:32**
Original artifact	**Internet Explorer Main History**

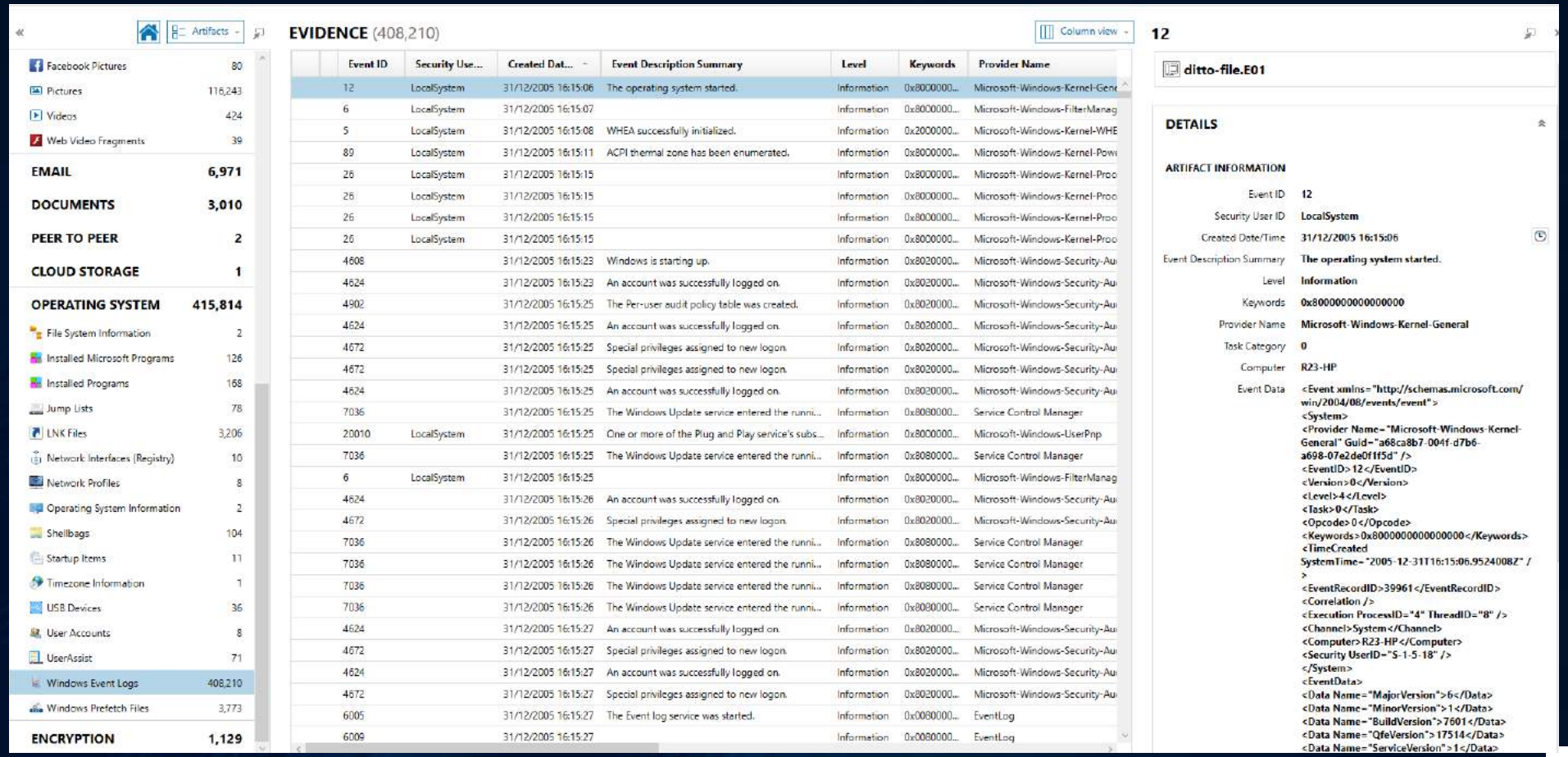
EVIDENCE INFORMATION

Source	**ditto-file.E01 - Partition 2 (Microsoft NTFS, 465.66 GB)\System Volume Information \{b9943ae3-7d6d-11e1-8b5b-74de2bc92906}{3808876b-c176-4e48-b7ae-04046e6cc752}**
Location	**File Offset 293131648**
Evidence number	**ditto-file.E01**

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI Hard Disk – AXIOM:



STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI Log del Join al dominio:

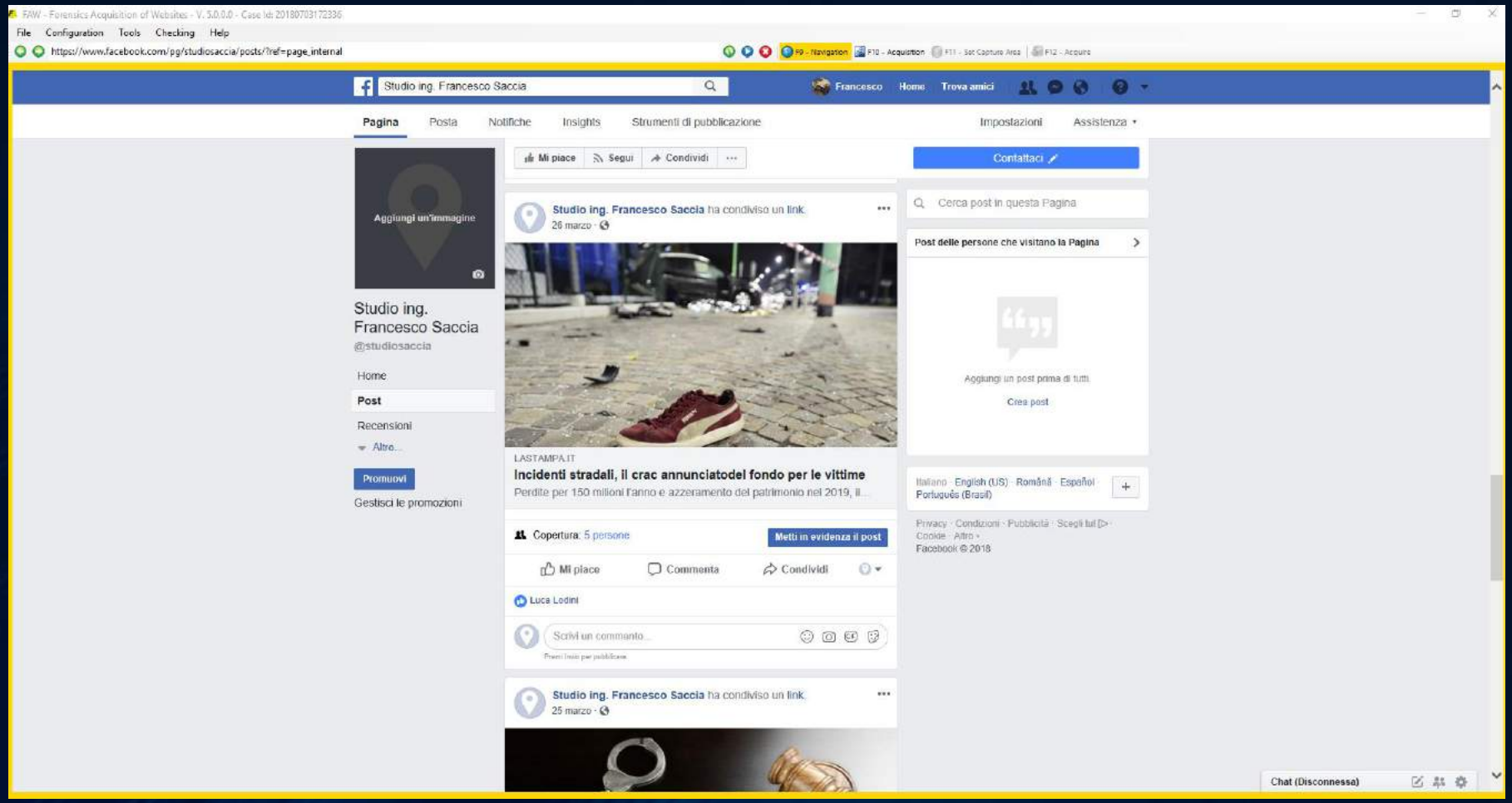
```
01/20 14:53:32 NetpChangeMachineName: from 'PI2SIN82' to 'PI2SIN49' using '[redacted]' [0x2]
01/20 14:53:32 NetpDsGetDcName: trying to find DC in domain 'ASLTO3', flags: 0x1020
01/20 14:53:32 NetpDsGetDcName: found DC '\\AD-AGN' in the specified domain
01/20 14:53:32 NetpChangeMachineName: status of connecting to  dc '\\AD-AGN': 0x0
01/20 14:53:32 NetpGetLsaPrimaryDomain: status: 0x0
01/20 14:53:32 NetpManageMachineAccountWithSid: status of NetUserSetInfo on '\\AD-AGN' for 'PI2SIN82$': 0x0
01/20 14:53:32 NetpGetLsaPrimaryDomain: status: 0x0
01/20 14:53:32 NetpGetDnsHostName: PrimaryDnsSuffix defaulted to DNS domain name: ASLTO3.LOC
01/20 14:53:32 NetpGetComputerObjectDn: Cracking account name ASLTO3\PI2SIN49$ on \\AD-AGN
01/20 14:53:32 NetpGetComputerObjectDn: Crack results:  (Account already exists) DN = CN=PI2SIN49,OU=Sede,OU=Client,OU=Pinerolo,OU=Objetcs,DC=ASLTO3,DC=LOC
01/20 14:53:32 NetpModifyComputerObjectInDs: Initial attribute values:
01/20 14:53:32          DnsHostName  =  PI2SIN49.ASLTO3.LOC
01/20 14:53:32          ServicePrincipalName  =  HOST/PI2SIN49.ASLTO3.LOC  HOST/PI2SIN49
01/20 14:53:32 NetpModifyComputerObjectInDs: Computer Object already exists in OU:
01/20 14:53:32          DnsHostName  =  PI2SIN82.ASLTO3.LOC
01/20 14:53:32          ServicePrincipalName  =  HOST/PI2SIN49  HOST/PI2SIN82.ASLTO3.LOC
01/20 14:53:32 NetpModifyComputerObjectInDs: Attribute values to set:
01/20 14:53:32          DnsHostName  =  PI2SIN49.ASLTO3.LOC
01/20 14:53:32          ServicePrincipalName  =  HOST/PI2SIN49.ASLTO3.LOC
01/20 14:53:32 ldap_unbind status: 0x0
01/20 14:53:32 NetpChangeMachineName: status of setting DnsHostName and SPN: 0x0
01/20 14:53:32 NetpChangeMachineName: status of setting DnsHostName and SPN: 0x0
```

```
01/20 15:16:37 NetpChangeMachineName: from 'PI2SIN49' to 'PI2SIN142' using '[redacted]' [0x2]
01/20 15:16:37 NetpDsGetDcName: trying to find DC in domain 'ASLTO3', flags: 0x1020
01/20 15:16:37 NetpDsGetDcName: found DC '\\AD-PINEROLO-1' in the specified domain
01/20 15:16:37 NetpChangeMachineName: status of connecting to  dc '\\AD-PINEROLO-1': 0x0
01/20 15:16:37 NetpGetLsaPrimaryDomain: status: 0x0
01/20 15:16:37 NetpManageMachineAccountWithSid: status of NetUserSetInfo on '\\AD-PINEROLO-1' for 'PI2SIN49$': 0x0
01/20 15:16:37 NetpGetLsaPrimaryDomain: status: 0x0
01/20 15:16:37 NetpGetDnsHostName: PrimaryDnsSuffix defaulted to DNS domain name: ASLTO3.LOC
01/20 15:16:37 NetpGetComputerObjectDn: Cracking account name ASLTO3\PI2SIN142$ on \\AD-PINEROLO-1
01/20 15:16:37 NetpGetComputerObjectDn: Crack results:  (Account already exists) DN = CN=PI2SIN142,OU=Sede,OU=Client,OU=Pinerolo,OU=Objetcs,DC=ASLTO3,DC=LOC
01/20 15:16:37 NetpModifyComputerObjectInDs: Initial attribute values:
01/20 15:16:37          DnsHostName  =  PI2SIN142.ASLTO3.LOC
01/20 15:16:37          ServicePrincipalName  =  HOST/PI2SIN142.ASLTO3.LOC  HOST/PI2SIN142
01/20 15:16:37 NetpModifyComputerObjectInDs: Computer Object already exists in OU:
01/20 15:16:37          DnsHostName  =  PI2SIN49.ASLTO3.LOC
01/20 15:16:37          ServicePrincipalName  =  HOST/PI2SIN142  HOST/PI2SIN49.ASLTO3.LOC
01/20 15:16:37 NetpModifyComputerObjectInDs: Attribute values to set:
01/20 15:16:37          DnsHostName  =  PI2SIN142.ASLTO3.LOC
01/20 15:16:37          ServicePrincipalName  =  HOST/PI2SIN142.ASLTO3.LOC
01/20 15:16:37 ldap_unbind status: 0x0
01/20 15:16:37 NetpChangeMachineName: status of setting DnsHostName and SPN: 0x0
```

STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ACQUISIZIONE DA WEB con FAW - FACEBOOK:



STUDIO SACCIA

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ACQUISIZIONE DA WEB con FAW - FACEBOOK:

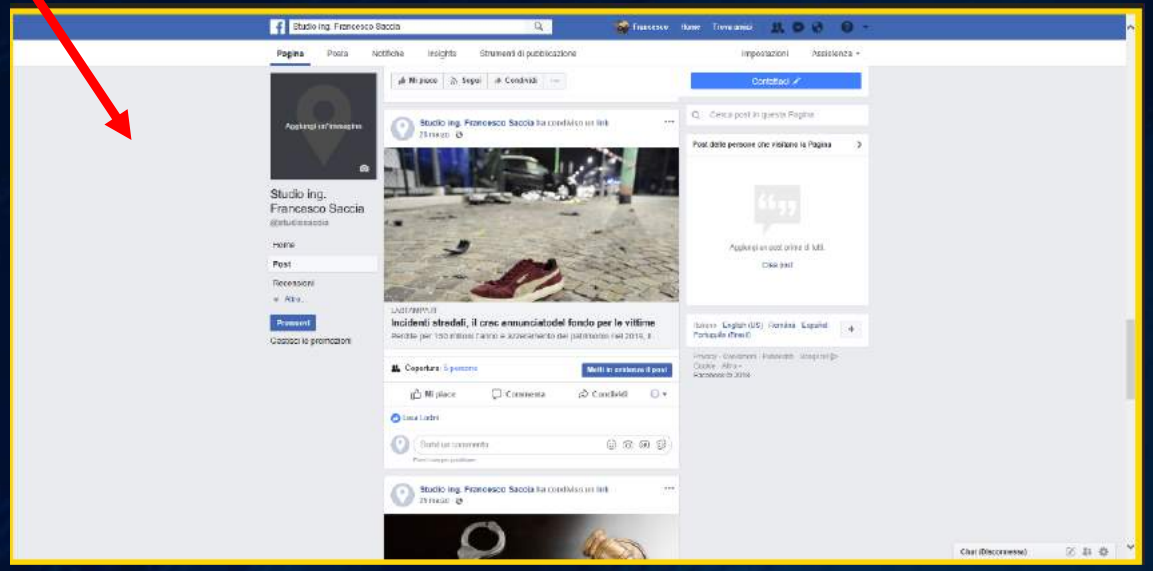
Nome	Ultima modifica	Tipo	Dimensione
ImagesA4	03/07/2018 17:25	Cartella di file	
Objects	03/07/2018 17:25	Cartella di file	
Acquisition	03/07/2018 17:25	Documento di testo	5 KB
Acquisition	03/07/2018 17:25	Documento di testo	4 KB
Acquisition	03/07/2018 17:25	Documento XML	8 KB
Checking.faw	03/07/2018 17:25	File FAW	1 KB
Code	03/07/2018 17:25	Documento HTML	1.712 KB
CodeFrame	03/07/2018 17:25	Documento HTML	1 KB
Headers	03/07/2018 17:25	Documento di testo	1 KB
hosts	16/07/2016 13:45	File	1 KB
Image	03/07/2018 17:25	File PNG	485 KB
SystemLogEvents	03/07/2018 17:25	Documento di testo	4 KB

Acquisition - Blocco note

File Modifica Formato Visualizza ?

```
URL: https://www.facebook.com/pg/studiosaccia/posts/?ref=page_internal
Host: www.facebook.com
IP Host: 31.13.86.38
User Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko
Capture Date/Time start UTC: 2018-07-03T15:25:21
Capture Date/Time end UTC: 2018-07-03T15:25:28
Capture Date/Time start computer time: 2018-07-03T17:25:21+0200
Capture Date/Time end computer time: 2018-07-03T17:25:28+0200
Network avaible id: 107B44A56DC3 name: Ethernet
Network avaible id: 005056C00001 name: VMware Network Adapter VMnet1
Network avaible id: 005056C00008 name: VMware Network Adapter VMnet8
Network avaible id:  name: Loopback Pseudo-Interface 1
Ntp Server: Local machine
Is in use proxy:  False
Proxy: www.google.com
DNS Local Machine 91.80.35.134
ExternalIpMachine:
Case ID: 20180703172336
Acquisition ID:  20180703172336#00001
Detective: ing. Saccia


Image.png
================================================================================
Hash MD5 : 99b9ac196cfcc05b27afb0615049b9d5
Hash SHA1: f06b45e9672dd97fe939506ec6f02eded20923aa
Width : 1919px
Height : 942px
```



STUDIO SACCIA

Grazie per l'attenzione