

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

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.

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

PRODUZIONE PROVE DIGITALI:

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

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

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



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

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



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

REPORT ACQUISIZIONE Hard Disk:

Physical Image E01:

Target File Name: HDD_HITACHI_SN_X0GNSUMR

Image File Segment Size: 2147483648

Source HPA/DCO: Indicate Only

Buffer Size: 1M

Error Granularity:

Swap Byte Pairs of the Media Data: Disabled

Compression Type: Empty Block

EWFF File Format: encase6

Read Error Retries:

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

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

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



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI SMARTPHONE – UFED:

Reader File View Tools Report Help

All Projects

Welcome Extraction Summary (1)

All Content Physical

Extraction Summary

+ Add extraction Project settings Generate report

Extractions: 1

Physical Samsung GSM SM-G920F Galaxy S6
Fisica [ADB Rooted]

Extraction start date/time: 08/11/2016 08:47:37
Extraction end date/time: 08/11/2016 13:16:11
\\LEONARDO\Analisi Informatiche\16-2-2...

Case Information
Case number: 2232/16

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/zerofftoss/zerofftoss.0.1/MMB29K/G920FX...
Detected Phone Vendor	samsung
Factory Number	R58G306TCUJ
IMEI	357558064019819
ICCID	8939883262002046745
Auto Time Zone	True
Auto Time	True
Indirizzo MAC Bluetooth	60AF6D508502
Tethering	
Name AP hotspot	AndroidAP
Password hotspot	bek6149

Examiner name: SACCIA Francesco

Device Content

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 (5)	User Accounts	14 (1)	User Dictionary	373
Web History	17 (2)	Wireless Networks	1		

Data Files

Applications	2626 (176)	Audio	117	Configurations	46 (1)
Databases	357	Documents	3	Images	3289 (21)
Text	1407 (240)	Videos	90 (5)		

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	



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE
ANALISI SMARTPHONE – UFED:

[illegible]

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

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



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI SMARTPHONE – UFED:

Reader File View Tools Report Help

Welcome x Extraction Summary (1) x Timeline (9531) x

Timeline (9531)

Table View Graphic View

Table Search

		#	Type	Timestamp	Party	Description	Source file information
	☒	4485	Web History	01/12/2016 02:19:33(UTC+1)		Katsuni Porn Videos & XXX Movie...	
	☒	4486	Web History	01/12/2016 02:19:44(UTC+1)		Katsuni Porn Videos & XXX Movie...	
	☒	4487	Web History	01/12/2016 02:19:54(UTC+1)		Katsuni gets It Up Her Ass! - Free...	
	☒	4488	Log Entries	01/12/2016 19:23:46(UTC+1)		Wifi In0 Wifi Out0 Wan In0 Wan...	
	☒	4489	Device Notificati...	01/12/2016 21:08:28(UTC+1)		Immobiliare.it 1 annuncio per l...	
02/12/2016 (2)							
	☒	4490	SMS Messages	02/12/2016 08:41:29(UTC+1)	From: +393341551470...	Io non tanto bene mi è venuta la f...	
	☒	4491	Device Notificati...	02/12/2016 22:23:48(UTC+1)		Immobiliare.it 1 annuncio per l...	
03/12/2016 (8)							
	☒	4492	SMS Messages	03/12/2016 08:06:51(UTC+1)		Vodafone Rete Sicura si rinnova il...	
	☒	4493	Log Entries	03/12/2016 08:07:16(UTC+1)		AutoScout24: Wifi In0 Wifi Out0...	
	☒	4494	SMS Messages	03/12/2016 08:21:26(UTC+1)		Grazie per la ricarica da 10.00 eur...	
	☒	4495	SMS Messages	03/12/2016 09:03:32(UTC+1)	From: 421009	Vodafone VITAMINAI Scegli tra IN...	
	☒	4496	Call Log	03/12/2016 12:10:11(UTC+1)	From: 393463546850@s... To: 393491436588@swh...	00:00:00	
	☒	4497	Instant Messages	03/12/2016 12:40:53(UTC+1)	From: 100000642073796		
	☒	4498	Log Entries	03/12/2016 15:20:16(UTC+1)		MobileSafari: Wifi In0 Wifi Out0...	
	☒	4499	Contacts	03/12/2016 18:29:39(UTC+1)		Ozzero	
04/12/2016 (2)							
	☒	4500	Call Log	04/12/2016 11:33:14(UTC+1)	From: 393457065899@s... To: 393463546850@swh...	00:00:00	
	☒	4501	Call Log	04/12/2016 14:08:39(UTC+1)	From: 393463546850@s...	00:00:00	

SMS Message

Source:

SMSC:

Folder: Inbox

Timestamp: 03/12/2016 08:21:26(UTC+1)

Delivered:

Read: 03/12/2016 08:25:02(UTC+1)

Status: Read

Extraction: File System

Source file:

All timestamps

Parties

Body

Grazie per la ricarica da 10.00 euro. Per verificare credito e contatori chiama il 414 o vai sull'app My Vodafone. Scopri le offerte per te al 40333



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI SMARTPHONE – UFED:

The screenshot displays the UFED Reader interface. The left sidebar shows a tree view of analyzed data, including 'Locations (710)'. The main window shows a table of locations with columns for Origin, Timestamp, End Time, Position, and Map Address. A red arrow points from a specific location in the table to a Google Maps view of the same location.

Origin	Timestamp	End Time	Position	Map Address
	26/03/2017 18:26:32(UTC+2)		(45.139717, 8.455120)	
	26/03/2017 15:41:14		(45.128761, 8.457850)	
	26/03/2017 15:41:11		(45.128764, 8.457828)	
	26/03/2017 15:41:06		(45.128803, 8.457894)	
	26/03/2017 15:41:05		(45.128589, 8.457886)	
	26/03/2017 15:41:15(UTC+2)		(45.128761, 8.457850)	
	26/03/2017 15:41:11(UTC+2)		(45.128764, 8.457828)	
	26/03/2017 15:41:07(UTC+2)		(45.128803, 8.457895)	
	26/03/2017 15:41:05(UTC+2)		(45.128589, 8.457887)	
	25/03/2017 22:12:15		(45.140817, 8.451464)	
	25/03/2017 22:12:16(UTC+1)		(45.140817, 8.451463)	
			(45.131875, 8.458244)	
			(45.131875, 8.458244)	
			(45.131875, 8.458244)	
			(45.131875, 8.458244)	
			(45.131875, 8.458244)	
			(45.132011, 8.458222)	
			(45.132011, 8.458222)	
			(45.132011, 8.458222)	
			(45.132011, 8.458222)	
			(45.131900, 8.458200)	
			(45.131900, 8.458200)	

The Google Maps view shows the location (45.128761, 8.457850) in Casale Monferrato, Italy. The map is titled 'Mappa per 45.128761, 8.457850'.

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI Hard Disk – AXIOM:

Magnet AXIOM Examine v12.5.8637 - 25224/15 RGNR

File Tools Process Help

FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone Media categories

Artifacts

EVIDENCE (606,445)

Column view

Item	Type	Category	Date and time
6	Windows Event Logs	Operating System	31/08/2015 10:55:46
1016	Windows Event Logs	Operating System	30/06/2016 10:02:27
7036	Windows Event Logs	Operating System	12/01/2017 17:02:00
22	Windows Event Logs	Operating System	21/02/2017 10:55:53
3	Windows Event Logs	Operating System	23/06/2015 13:51:53
11724	Windows Event Logs	Operating System	16/07/2011 04:48:12
100	Windows Event Logs	Operating System	08/06/2016 08:14:54
7036	Windows Event Logs	Operating System	03/03/2011 10:42:57
0	Windows Event Logs	Operating System	18/11/2015 11:24:40
42	Windows Event Logs	Operating System	07/09/2017 12:12:41
8212	Windows Event Logs	Operating System	16/11/2015 10:21:08
100	Windows Event Logs	Operating System	24/05/2017 08:54:05
7036	Windows Event Logs	Operating System	27/06/2016 14:13:17
0	Windows Event Logs	Operating System	15/02/2014 06:12:29
21	Windows Event Logs	Operating System	30/11/2014 07:55:53
7036	Windows Event Logs	Operating System	16/09/2011 18:03:25
51047	Windows Event Logs	Operating System	17/07/2011 01:00:34
7036	Windows Event Logs	Operating System	03/03/2011 07:05:02
4624	Windows Event Logs	Operating System	26/05/2011 23:49:55
4624	Windows Event Logs	Operating System	17/05/2011 07:24:26
6013	Windows Event Logs	Operating System	09/01/2017 10:44:28
4624	Windows Event Logs	Operating System	06/07/2016 09:17:47
701	Windows Event Logs	Operating System	14/05/2015 11:07:16
100	Windows Event Logs	Operating System	03/10/2016 09:07:15
7036	Windows Event Logs	Operating System	16/09/2011 17:40:57
4624	Windows Event Logs	Operating System	14/10/2015 13:47:33
4624	Windows Event Logs	Operating System	02/02/2015 18:06:54
2005	Windows Event Logs	Operating System	25/09/2017 09:52:27
7036	Windows Event Logs	Operating System	31/05/2017 09:46:50
6009	Windows Event Logs	Operating System	24/01/2011 00:01:25
300	Windows Event Logs	Operating System	07/07/2015 11:51:40

ALL EVIDENCE 606,445

REFINED RESULTS 8,053

WEB RELATED 52,893

CHAT 768

SOCIAL NETWORKING 97

MEDIA 117,707

EMAIL 6,971

- EMail Files 36
- Outlook Appointments 218
- Outlook Contacts 6,717

DOCUMENTS 3,010

- Excel Documents 82
- Hangul Word Processor 1
- PDF Documents 360
- PowerPoint Documents 39
- RTF Documents 1,548
- Text Documents 893
- Word Documents 97

PEER TO PEER 2

CLOUD STORAGE 1

OPERATING SYSTEM 415,814

ENCRYPTION 1,129

PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI Hard Disk – AXIOM:

ALL EVIDENCE	251,184	Search Term	URL	Date/Time	Date/Ti...	Original...
REFINED RESULTS	1,866	hp driver	http://www.google.it/url?sa=t&rct=j&q=hp+driver...	03/03/2012 08:49:36		
Classifieds URLs	2	all	http://www.google.it/s?hl=it&sugexp=frgbl&gs_nf...	03/04/2012 13:33:41		
Dating Sites URLs	8	speed test	http://www.google.it/#hl=it&sugexp=llsin&gs_nf=1...			spee
Facebook URLs	98	medicina	http://www.google.it/s?hl=it&gs_rm=7&gs_ri=psy-a...	26/03/2013 11:37:33		
Google Analytics First Visit Cookies	15	medicin	http://www.google.it/s?hl=it&gs_rm=7&gs_ri=psy-a...	26/03/2013 11:37:32		
Google Analytics Referral Cookies	16	easyjet	http://www.google.it/url?sa=t&rct=j&q=easyjet&so...			
Google Analytics Session Cookies	15	mess	http://www.google.it/s?hl=it&gs_nf=1&cp=4&gs_id...	03/03/2012 14:42:40		
Google Analytics URLs	52	previsioni meteo torino	http://www.google.it/search?hl=it&client=psy-ab&...	22/05/2012 09:48:58		previ
Google Maps Queries	64	speed test	http://www.google.it/url?sa=f&rct=j&url=http://ww...	03/04/2012 09:58:30		
Google Searches	763	medicina anti	http://www.google.es/s?hl=it&gs_rm=7&gs_ri=psy-a...	26/03/2013 11:07:04		
Google Translate	44	al	http://www.google.it/s?hl=it&sugexp=frgbl&gs_nf...	03/04/2012 13:33:41		
Identifiers	357	previsio	http://www.google.it/s?hl=it&gs_nf=1&cp=8&gs_id...	29/05/2012 12:14:34		
Malware/Phishing URLs	7	easyjet	http://www.google.it/?gws_rd=cr#gs_rm=23&gs_ri=...			ea
Rebuilt Webpages	321	al	http://www.google.it/s?hl=it&sugexp=frgbl&gs_nf...	03/04/2012 13:33:41		
Social Media URLs	96	previsi	http://www.google.it/s?hl=it&sugexp=frgbl&gs_nf...	11/04/2012 15:42:58		
Tax Site URLs	8	pr	http://www.google.it/s?hl=it&gs_nf=1&cp=2&gs_id...	22/05/2012 09:51:00		
WEB RELATED	32,659	medicina egizia storia	http://www.google.it/search?hl=it&client=psy-ab&...	26/03/2013 10:55:59		medicina egiz
Chrome Archived Web History	19	messentools	http://www.google.it/#hl=it&gs_nf=1&cp=7&gs_id...	03/03/2012 14:42:44		messent
Chrome Autofill	1	speed test	http://www.google.it/url?sa=f&rct=j&url=http://ww...			
Chrome Cache Records	794	previsioni meteo p	http://www.google.it/s?hl=it&gs_nf=3&cp=18&gs_i...	14/11/2012 09:44:05		
Chrome Cookies	89	previsioni	http://www.google.it/s?hl=it&sugexp=frgbl&gs_nf...	11/04/2012 15:43:00		
Chrome Current Session	13	medicina an	http://www.google.es/s?hl=it&gs_rm=7&gs_ri=psy-a...	26/03/2013 11:07:00		
Chrome Current Tabs	6	allergia al	http://www.google.it/s?hl=it&sugexp=frgbl&gs_nf...	03/04/2012 13:33:51		
Chrome Downloads	4	allergia al ta	http://www.google.it/s?hl=it&sugexp=frgbl&gs_nf...	03/04/2012 13:33:54		
Chrome Favicons	11	t	http://www.google.it/s?hl=it&gs_nf=1&cp=1&gs_id...	22/05/2012 09:46:14		
Chrome History Index	7	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=frgbl&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.qooqle.it/s?hl=it&sugexp=frqbl&qs_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%2Ffit%2Fit%2Fsupport-drivers.html&ei=HNtRT6azlsbxsgb5opTOCw&usq=AFQjCNHMRNRIEeXOW6gfp7bdyLfN0COMmeA

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



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI Hard Disk – AXIOM:

Artifacts - EVIDENCE (408,210) Column view

Facebook Pictures 80
Pictures 116,243
Videos 424
Web Video Fragments 39

EMAIL 6,971
DOCUMENTS 3,010
PEER TO PEER 2
CLOUD STORAGE 1

OPERATING SYSTEM 415,814

- File System Information 2
- Installed Microsoft Programs 126
- Installed Programs 168
- Jump Lists 78
- LNK Files 3,206
- Network Interfaces (Registry) 10
- Network Profiles 8
- Operating System Information 2
- Shellbags 104
- Startup Items 11
- Timezone Information 1
- USB Devices 36
- User Accounts 8
- UserAssist 71
- Windows Event Logs 408,210
- Windows Prefetch Files 3,773

ENCRYPTION 1,129

Event ID	Security Use...	Created Date	Event Description Summary	Level	Keywords	Provider Name
12	LocalSystem	31/12/2005 16:15:06	The operating system started.	Information	0x80000000...	Microsoft-Windows-Kernel-Gen...
6	LocalSystem	31/12/2005 16:15:07		Information	0x80000000...	Microsoft-Windows-FilterManag
5	LocalSystem	31/12/2005 16:15:08	WHEA successfully initialized.	Information	0x20000000...	Microsoft-Windows-Kernel-WHE
89	LocalSystem	31/12/2005 16:15:11	ACPI thermal zone has been enumerated.	Information	0x80000000...	Microsoft-Windows-Kernel-Powi
26	LocalSystem	31/12/2005 16:15:15		Information	0x80000000...	Microsoft-Windows-Kernel-Proo
26	LocalSystem	31/12/2005 16:15:15		Information	0x80000000...	Microsoft-Windows-Kernel-Proo
26	LocalSystem	31/12/2005 16:15:15		Information	0x80000000...	Microsoft-Windows-Kernel-Proo
4608		31/12/2005 16:15:23	Windows is starting up.	Information	0x80200000...	Microsoft-Windows-Security-Au
4624		31/12/2005 16:15:23	An account was successfully logged on.	Information	0x80200000...	Microsoft-Windows-Security-Au
4902		31/12/2005 16:15:25	The Per-user audit policy table was created.	Information	0x80200000...	Microsoft-Windows-Security-Au
4624		31/12/2005 16:15:25	An account was successfully logged on.	Information	0x80200000...	Microsoft-Windows-Security-Au
4672		31/12/2005 16:15:25	Special privileges assigned to new logon.	Information	0x80200000...	Microsoft-Windows-Security-Au
4672		31/12/2005 16:15:25	Special privileges assigned to new logon.	Information	0x80200000...	Microsoft-Windows-Security-Au
4624		31/12/2005 16:15:25	An account was successfully logged on.	Information	0x80200000...	Microsoft-Windows-Security-Au
7036		31/12/2005 16:15:25	The Windows Update service entered the runni...	Information	0x80800000...	Service Control Manager
20010	LocalSystem	31/12/2005 16:15:25	One or more of the Plug and Play service's subs...	Information	0x80000000...	Microsoft-Windows-UserPnp
7036		31/12/2005 16:15:25	The Windows Update service entered the runni...	Information	0x80800000...	Service Control Manager
6	LocalSystem	31/12/2005 16:15:25		Information	0x80000000...	Microsoft-Windows-FilterManag
4624		31/12/2005 16:15:26	An account was successfully logged on.	Information	0x80200000...	Microsoft-Windows-Security-Au
4672		31/12/2005 16:15:26	Special privileges assigned to new logon.	Information	0x80200000...	Microsoft-Windows-Security-Au
7036		31/12/2005 16:15:26	The Windows Update service entered the runni...	Information	0x80800000...	Service Control Manager
7036		31/12/2005 16:15:26	The Windows Update service entered the runni...	Information	0x80800000...	Service Control Manager
7036		31/12/2005 16:15:26	The Windows Update service entered the runni...	Information	0x80800000...	Service Control Manager
7036		31/12/2005 16:15:26	The Windows Update service entered the runni...	Information	0x80800000...	Service Control Manager
4624		31/12/2005 16:15:27	An account was successfully logged on.	Information	0x80200000...	Microsoft-Windows-Security-Au
4672		31/12/2005 16:15:27	Special privileges assigned to new logon.	Information	0x80200000...	Microsoft-Windows-Security-Au
4624		31/12/2005 16:15:27	An account was successfully logged on.	Information	0x80200000...	Microsoft-Windows-Security-Au
4672		31/12/2005 16:15:27	Special privileges assigned to new logon.	Information	0x80200000...	Microsoft-Windows-Security-Au
6005		31/12/2005 16:15:27	The Event log service was started.	Information	0x00800000...	EventLog
6009		31/12/2005 16:15:27		Information	0x00800000...	EventLog

12 ditto-file.E01

DETAILS

ARTIFACT INFORMATION

Event ID 12
Security User ID LocalSystem
Created Date/Time 31/12/2005 16:15:06
Event Description Summary The operating system started.
Level Information
Keywords 0x8000000000000000
Provider Name Microsoft-Windows-Kernel-General
Task Category 0
Computer R23-HP
Event Data <?xml:lang="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Kernel-General" Guid="{a68ca8b7-004f-d7b6-a698-07e2de0f1f5d}" /><EventID>12</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2005-12-31T16:15:06.9524008Z" /><EventRecordID>39961</EventRecordID><Correlation /><Execution ProcessID="4" ThreadID="8" /><Channel>System</Channel><Computer>R23-HP</Computer><Security UserID="S-1-5-18" /></System><EventData><Data Name="MajorVersion">6</Data><Data Name="MinorVersion">1</Data><Data Name="BuildVersion">7601</Data><Data Name="QfeVersion">17514</Data><Data Name="ServiceVersion">1</Data>



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ANALISI Log del Join al dominio:

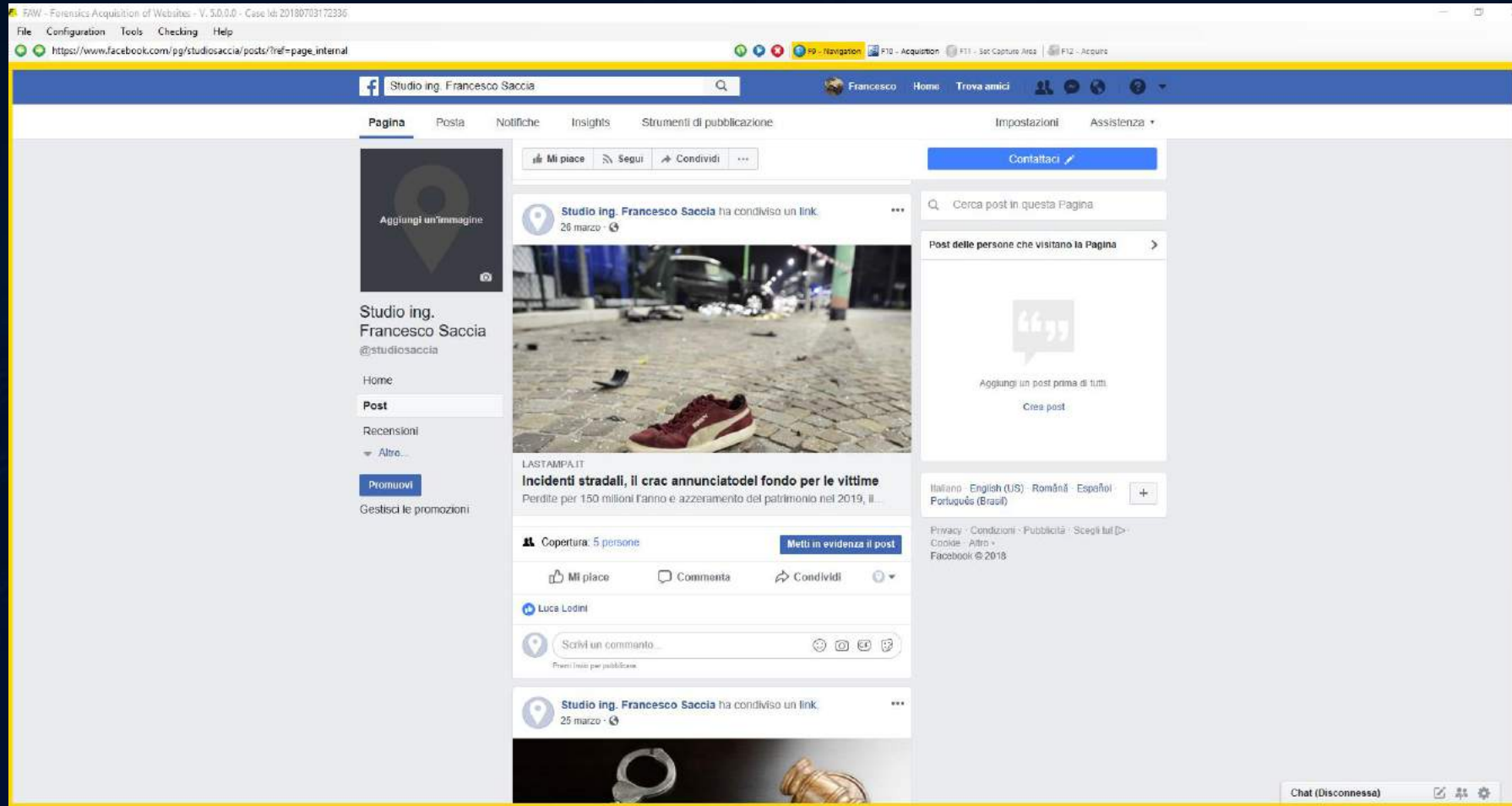
```
01/20 14:53:32 NetpChangeMachineName: from 'PI2SIN82' to 'PI2SIN49' using '[REDACTED]' [0x2]
01/20 14:53:32 NetpDsGetDcName: trying to find DC in domain 'ASLT03', flags: 0x1020
01/20 14:53:32 NetpDsGetDcName: found DC '\\AD-AGN' in the specified domain
01/20 14:53:32 NetpChangeMachineName: status 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$': 0x0
01/20 14:53:32 NetpGetLsaPrimaryDomain: status: 0x0
01/20 14:53:32 NetpGetDnsHostName: PrimaryDnsSuffix defaulted to DNS domain name: ASLT03.LOC
01/20 14:53:32 NetpGetComputerObjectDn: Cracking account name ASLT03\PI2SIN49$ 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=ASLT03,DC=LOC
01/20 14:53:32 NetpModifyComputerObjectInDs: Initial attribute values:
01/20 14:53:32     DnsHostName = PI2SIN49.ASLT03.LOC
01/20 14:53:32     ServicePrincipalName = HOST/PI2SIN49.ASLT03.LOC HOST/PI2SIN49
01/20 14:53:32 NetpModifyComputerObjectInDs: Computer Object already exists in OU:
01/20 14:53:32     DnsHostName = PI2SIN82.ASLT03.LOC
01/20 14:53:32     ServicePrincipalName = HOST/PI2SIN49 HOST/PI2SIN82.ASLT03.LOC
01/20 14:53:32 NetpModifyComputerObjectInDs: Attribute values to set:
01/20 14:53:32     DnsHostName = PI2SIN49.ASLT03.LOC
01/20 14:53:32     ServicePrincipalName = HOST/PI2SIN49.ASLT03.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 'ASLT03', 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$': 0x0
01/20 15:16:37 NetpGetLsaPrimaryDomain: status: 0x0
01/20 15:16:37 NetpGetDnsHostName: PrimaryDnsSuffix defaulted to DNS domain name: ASLT03.LOC
01/20 15:16:37 NetpGetComputerObjectDn: Cracking account name ASLT03\PI2SIN142$ 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=ASLT03,DC=LOC
01/20 15:16:37 NetpModifyComputerObjectInDs: Initial attribute values:
01/20 15:16:37     DnsHostName = PI2SIN142.ASLT03.LOC
01/20 15:16:37     ServicePrincipalName = HOST/PI2SIN142.ASLT03.LOC HOST/PI2SIN142
01/20 15:16:37 NetpModifyComputerObjectInDs: Computer Object already exists in OU:
01/20 15:16:37     DnsHostName = PI2SIN49.ASLT03.LOC
01/20 15:16:37     ServicePrincipalName = HOST/PI2SIN142 HOST/PI2SIN49.ASLT03.LOC
01/20 15:16:37 NetpModifyComputerObjectInDs: Attribute values to set:
01/20 15:16:37     DnsHostName = PI2SIN142.ASLT03.LOC
01/20 15:16:37     ServicePrincipalName = HOST/PI2SIN142.ASLT03.LOC
01/20 15:16:37 ldap_unbind status: 0x0
01/20 15:16:37 NetpChangeMachineName: status of setting DnsHostName and SPN: 0x0
```



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

ACQUISIZIONE DA WEB con FAW - FACEBOOK:



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

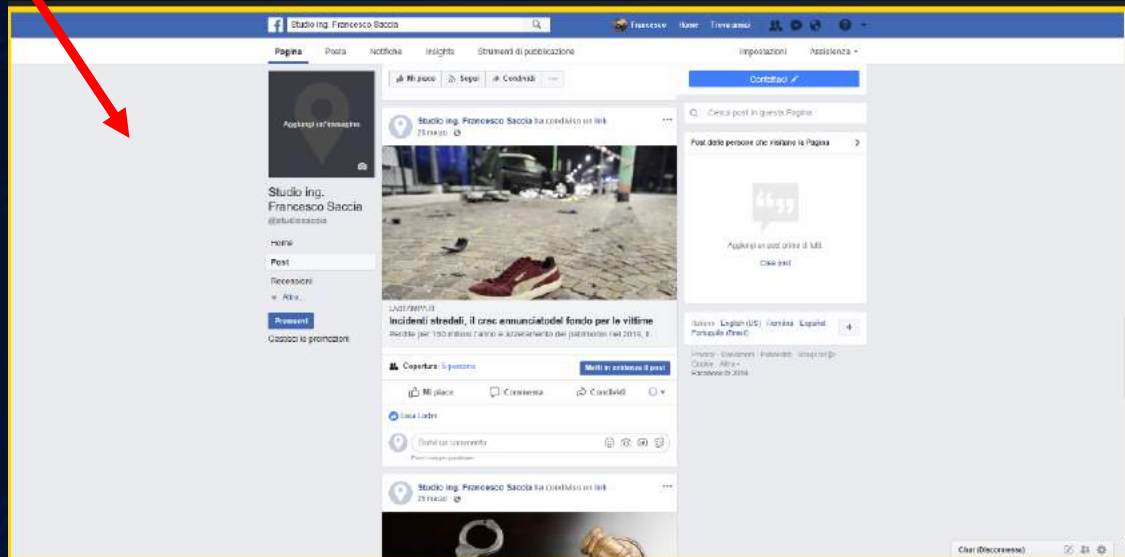
File Modifica Formato Visualizza ?

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 available id: 107B44A56DC3 name: Ethernet
Network available id: 005056C00001 name: VMware Network Adapter VMnet1
Network available id: 005056C00008 name: VMware Network Adapter VMnet8
Network available 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 : 99b9ac196cfc05b27afb0615049b9d5
Hash SHA1: f06b45e9672dd97fe939506ec6f02eded20923aa
Width : 1919px
Height : 942px



PROVE DIGITALI ED INFORMATICHE E PROCESSO CIVILE

Grazie per l'attenzione

WWW.STUDIOSACCIA.IT

