Che cosa sono i cookie: la verità su come gestirli, rimuoverli e difendere la privacy sul web

Ogni volta che ci colleghiamo con un sito Internet, il browser preleva automaticamente tutti gli elementi che compongono le pagine visualizzate e li salva in una cartella, sul disco fisso, che forma la cosiddetta **cache**. Il quantitativo di spazio occupato viene giustificato dalla **maggiore velocità di caricamento dei siti su cui si accede frequentemente**. Ogniqualvolta venga infatti richiesta la visualizzazione di un elemento contenuto in una pagina web, il browser verifica preventivamente se esso sia contenuto nella cache: in questo modo si può evitare che esso venga inutilmente riscaricato un'altra volta.

Oltre alla cache, il browser Internet memorizza, sul disco fisso, anche i **cookie** (in inglese, "*biscotto*") Si tratta di file di testo, di dimensioni estremamente compatte, la cui creazione è frequentemente richiesta da parte di un'applicazione web o di un normale sito Internet. La generazione del **cookie**, che avviene sempre fornendo tutte le necessarie istruzioni al browser web dell'utente, qualunque sia prodotto che egli stia impiegando, ha luogo sul sistema client ed il contenuto del **cookie viene reinviato all'applicazione web ogniqualvolta l'utente si connetta al medesimo server remoto**. I cookie consentono di annotare, sul sistema dell'utente che si collega ad un sito web, alcune informazioni successivamente utilizzabili, ad esempio, per evitare l'effettuazione di una nuova procedura di login.

Intorno al concetto di **cookie** hanno da sempre trovato terreno fertile credenze scorrette e falsi miti. Cerchiamo di far luce sull'argomento analizzando il **funzionamento dei cookie**, come possono essere utilizzati e le circostanze in cui essi possano rappresentare una potenziale minaccia.

Sgombriamo subito il campo dagli equivoci: trattandosi di semplici file testuali, i **cookie non rappresentano di per sé un pericolo**: anzi, il loro impiego è di fondamentale importanza, per esempio, per il corretto funzionamen-

to dei negozi online (i prodotti inseriti nel "carrello della spesa" vengono temporaneamente memorizzati in un cookie), per conservare il login in un blog, in un'area privata, in un forum, od in una qualunque applicazione web che richieda qualsiasi forma di autenticazione. I cookie sono utilizzati anche da aziende attive nel campo dell'advertising per tenere traccia del percorso seguito dagli utenti durante la visita di più siti Internet.
È proprio quest'ultimo punto quello che solitamente è fonte delle discussioni maggiori: le più grandi aziende attive nel campo della pubblicità sul web possono piazzare il loro codice su più siti Internet monitorando così, anche attraverso l'utilizzo di un cookie, a quali pagine uno stesso utente si sia connesso. Vi è mai successo di cercare informazioni, ad esempio, sulla disponibilità di un volo aereo da Roma a Parigi e, anche durante la navigazione su siti web che nulla hanno a che fare con i viaggi, trovare esposte informazioni pubblicitarie che fanno riferimento a tariffe aeree relative proprio alla tratta parigina? Potreste aver sperimentato una situazione analoga cercando il migliore albergo in una qualunque città del mondo oppure andando alla cerca del prezzo più conveniente di un dispositivo elettronico o di un elettrodomestico.
Com'è possibile che visitando altri siti web continuino ad esserci proposti prodotti strettamente correlati con i nostri interessi e le nostre precedenti ricerche?
La risposta è molto semplice ed ha a che fare proprio con i **cookie**. Quando si vive una situazione come quella appena illustrata, è assai probabile che si sia visitato almeno un sito Internet che ha richiesto la generazione (attraverso il codice in esso ospitato) di un cookie gestito dal dominio Internet di una stessa società. I siti web ove è stato memorizzato un codice analogo, attingeranno automaticamente al contenuto del cookie e, semplicemente, presenteranno le inserzioni di probabile maggior interesse per l'utente attingendo proprio alle informazioni tracciate nel file testuale.

La gestione di cookie è completamente dipendente dal browser web che si è deciso di impiegare: il programma che si utilizza per "navigare" in Rete può

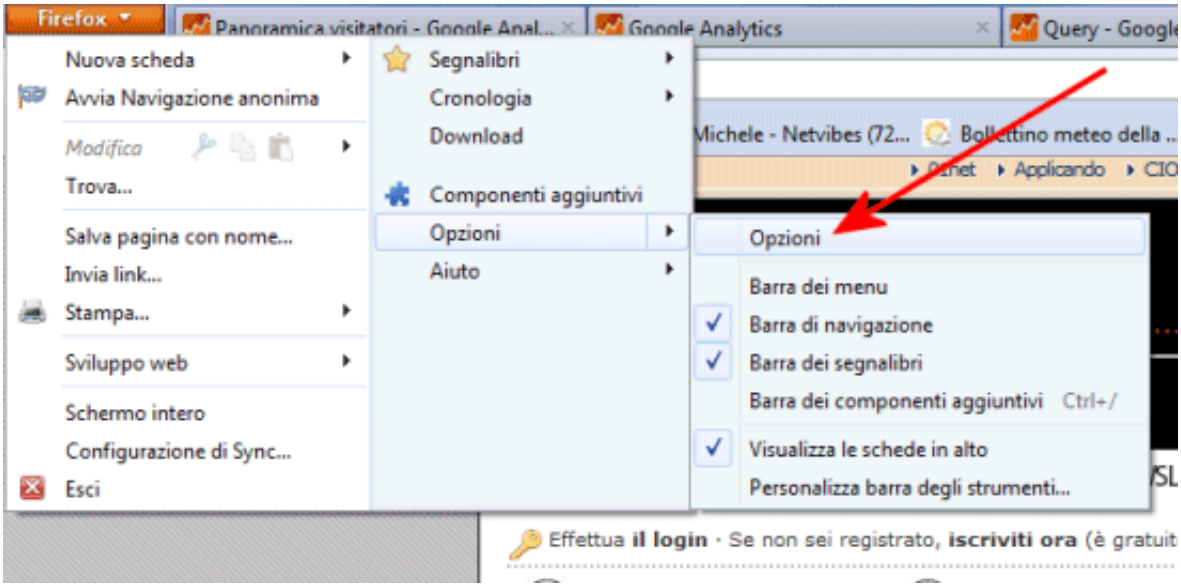
accettare i cookie, rifiutarli o limitarne l'uso solo a determinati siti. Il contenuto dei cookie può essere poi ovviamente eliminato ogniqualvolta lo si dovesse ritenere opportuno. Per procedere, è tipicamente necessario accedere alla finestra delle impostazioni del browser ed utilizzare l'apposita funzionalità di **rimozione dei cookie**. Tale strumento è di solito inserito nella medesima schermata attraverso la quale è possibile eliminare la *cache*.

Se un cookie è stato creato da un sito al quale si accede frequentemente e che prevede il controllo delle informazioni personali dell'utente, questo può contenere una password o un codice per la verifica dell'identità dell'utente stesso (si spera, in forma cifrata). Tali cookie non dovrebbero essere eliminati: è bene quindi aver cura di identificare gli eventuali cookie "utili" in modo da scongiurarne la rimozione ed evitare di dover reintrodurre manualmente tutte le informazioni in esse conservate. Altri cookie possono essere utilizzati per la memorizzazione delle preferenze e delle impostazioni personali per l'accesso a determinati siti web.

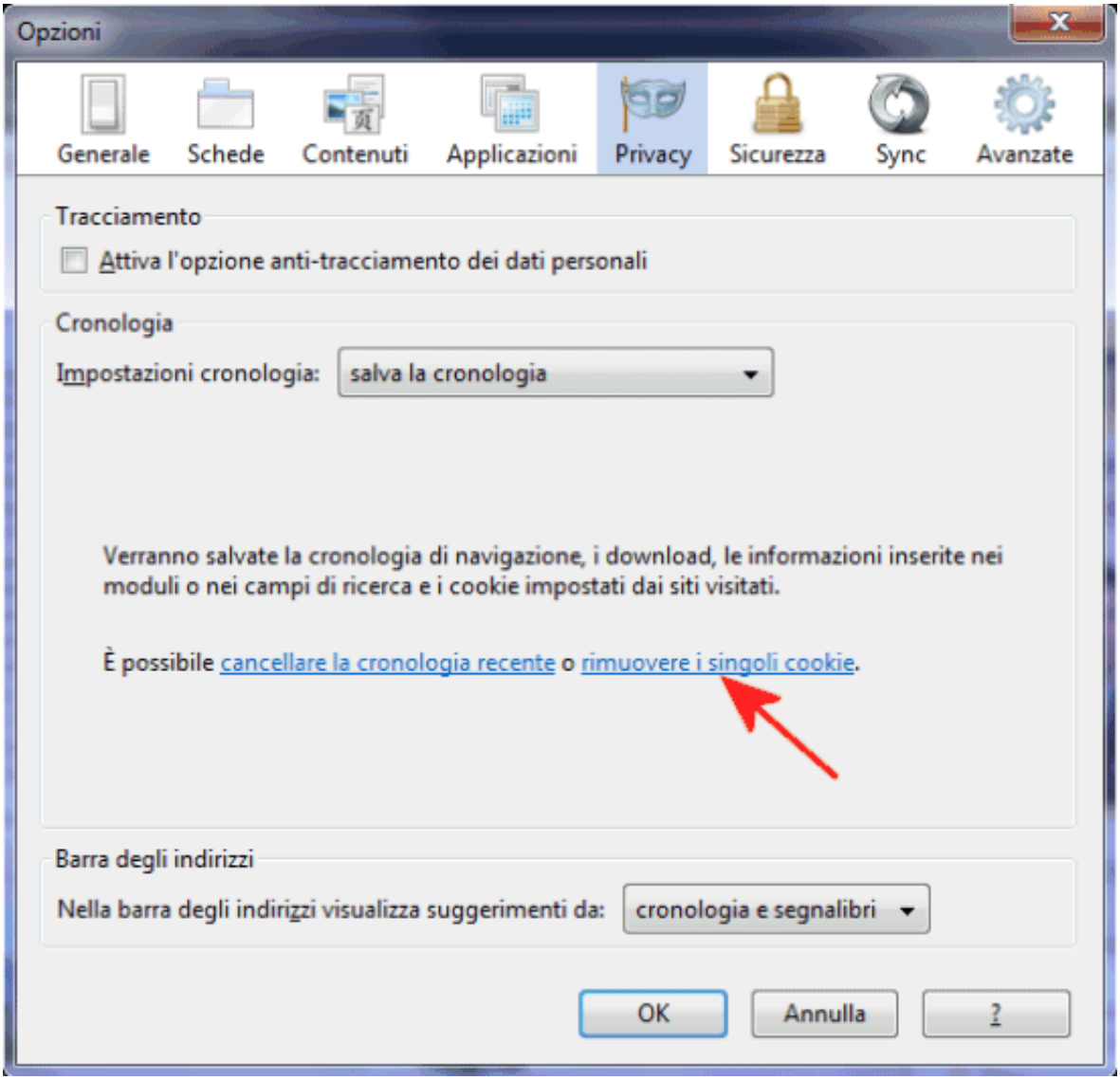
Gran parte dei siti, quindi, utilizzano i cookie per ottenere informazioni sulle precedenti visite all'interno dello stesso sito oppure per salvare, sul personal computer, **informazioni relative all'accesso ad aree del sito che necessitino dell'inserimento di un nome utente e di una password**. In questo modo l'utente non sarà costretto a reinserire nuovamente il nome utente e la password scelti: il sito Internet provvederà a verificare l'esistenza del cookie e a recuperarne il contenuto.

Gestire i cookie con i tre browser web più utilizzati

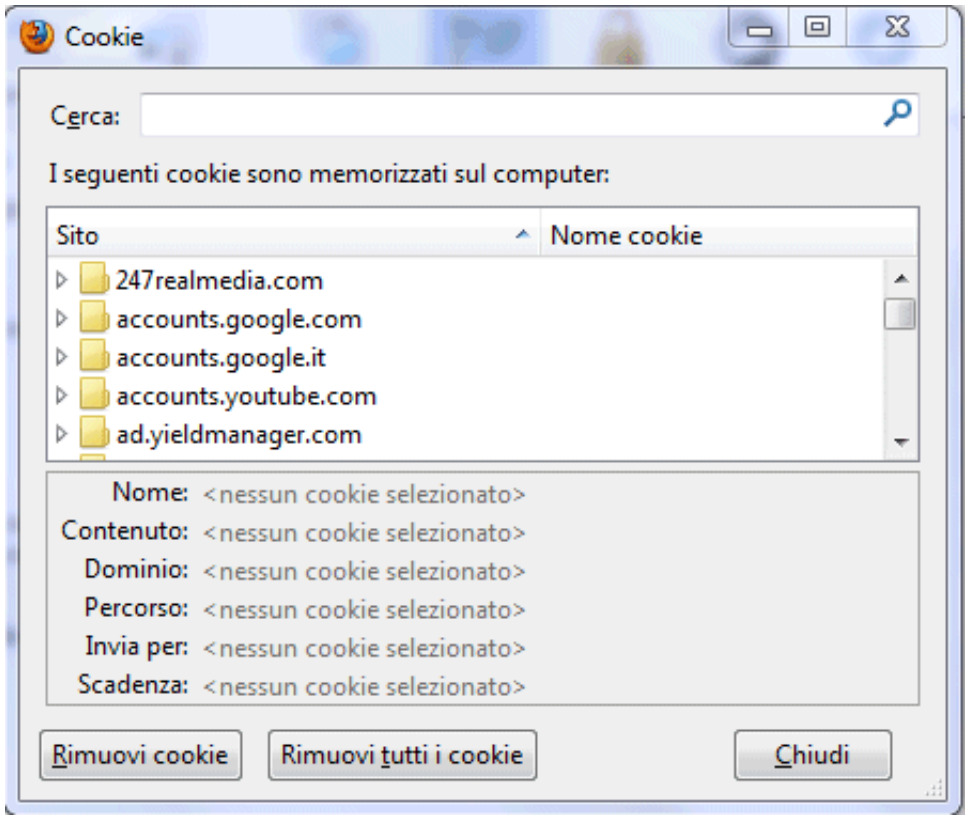
Iniziamo con Mozilla **Firefox.** Per accedere alla finestra che permette di rimuovere i cookie sin qui conservati sul personal computer, è necesario cliccare sul pulsante *Firefox* di colore arancione, in alto a sinistra nell'interfaccia del browser, selezionare *Opzioni* ed ancora una volta *Opzioni*:



Dopo aver selezionato la scheda prima *Privacy,* cliccando su *Rimuovi i singoli cookie,* si otterrà la lista dei cookie correntemente conservati sul sistema:

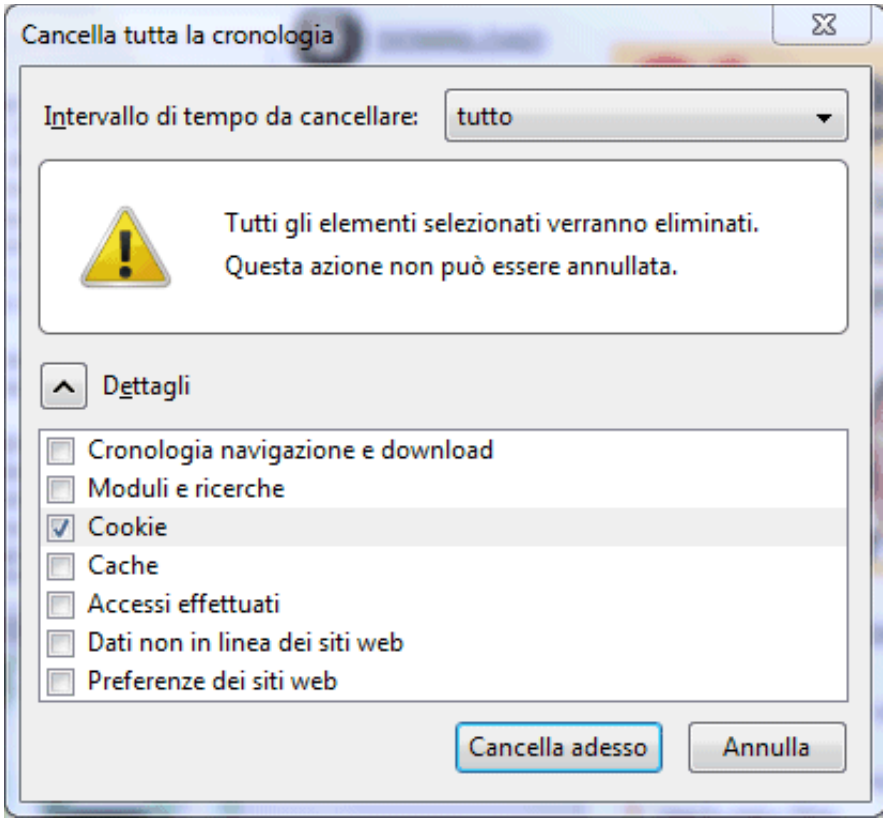


Per ogni sito web visitato, la schermata mostra il cookie memorizzato dal browser insieme con il suo contenuto:



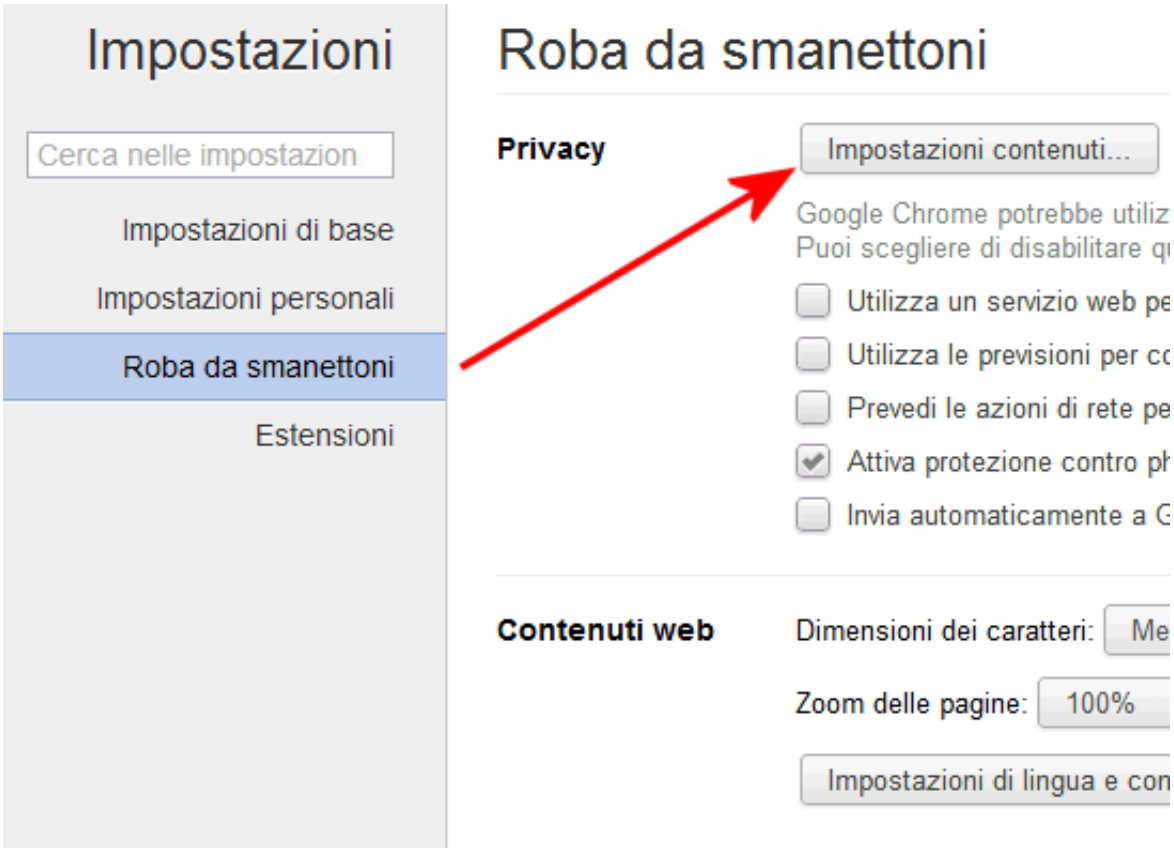
Nell'elenco si riconosceranno anche domini Internet che non si ricorda di aver mai visitato: si tratta di siti, generalmente gestiti da terze parti, che veicolano le inserzioni pubblicitarie presenti nelle pagine web o che s'incarino di elaborare analisi statistiche. I pulsanti *Rimuovi cookie* e *Rimuovi tutti i cookie* permetteranno di **eliminare il singolo cookie** selezionato oppure **cancellare tutte le informazioni memorizzate dal browser**.

Per rimuovere rapidamente tutti i cookie, in alternativa, è possibile – dalla finestra principale di Firefox – premere il tasto ALT, selezionare il menù *Strumenti*, la voce *Cancella la cronologia recente* ed attivare la casella *Cookie* scegliendo *tutto* dal menù a tendina *Intervallo di tempo da cancellare*:



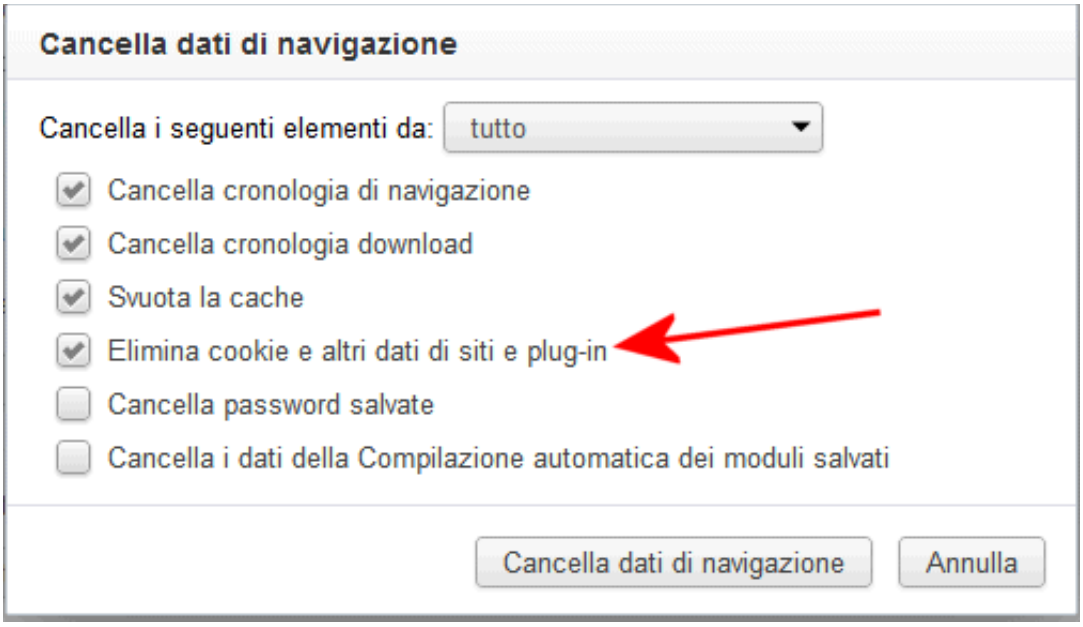
Da questa stessa finestra è possibile sbarazzarsi rapidamente della cronologia, della cache e di tutti gli altri dati via a via memorizzati dal browser web sul disco fisso.

La procedura da seguire nel caso di Google **Chrome** è sostanzialmente identica. Per procedere è necessario cliccare sull'icona a forma di "chiave inglese" posta accanto alla barra degli indirizzi e selezionare la voce *Impostazioni*. In alternativa, è possibile digitare chrome://settings nella barra degli URL di Chrome e premere il tasto Invio. Dalla sezione *Roba da smanettoni,* si deve cliccare sul pulsante *Impostazioni contenuti*:



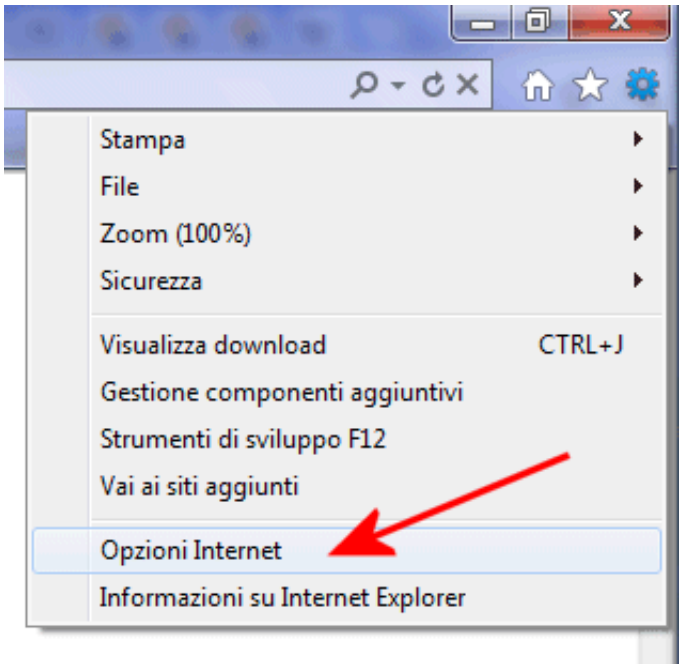
Cliccando, quindi, sul pulsante *Tutti i cookie e i dati dei siti*, Google Chrome mostrerà, in corrispondenza dell'indicazione di ciascun dominio visitato, il numero di cookie memorizzati in locale. Con pochi clic del mouse è possibile eventualmente esaminarne il contenuto.
Il pulsante *Rimuovi tutto* che campeggia in alto a destra, dà modo di **cancellare tutti i cookie** sin qui conservati sul sistema.

In alternativa, per **rimuovere i cookie** in modo diretto insieme con il loro contenuto, basterà fare clic sulla sezione *Roba da smanettoni*, fare clic sul pulsante *Cancella dati di navigazione* ed assicurarsi che sia spuntata la casella **Elimina cookie e altri dati di siti e plug-in**:

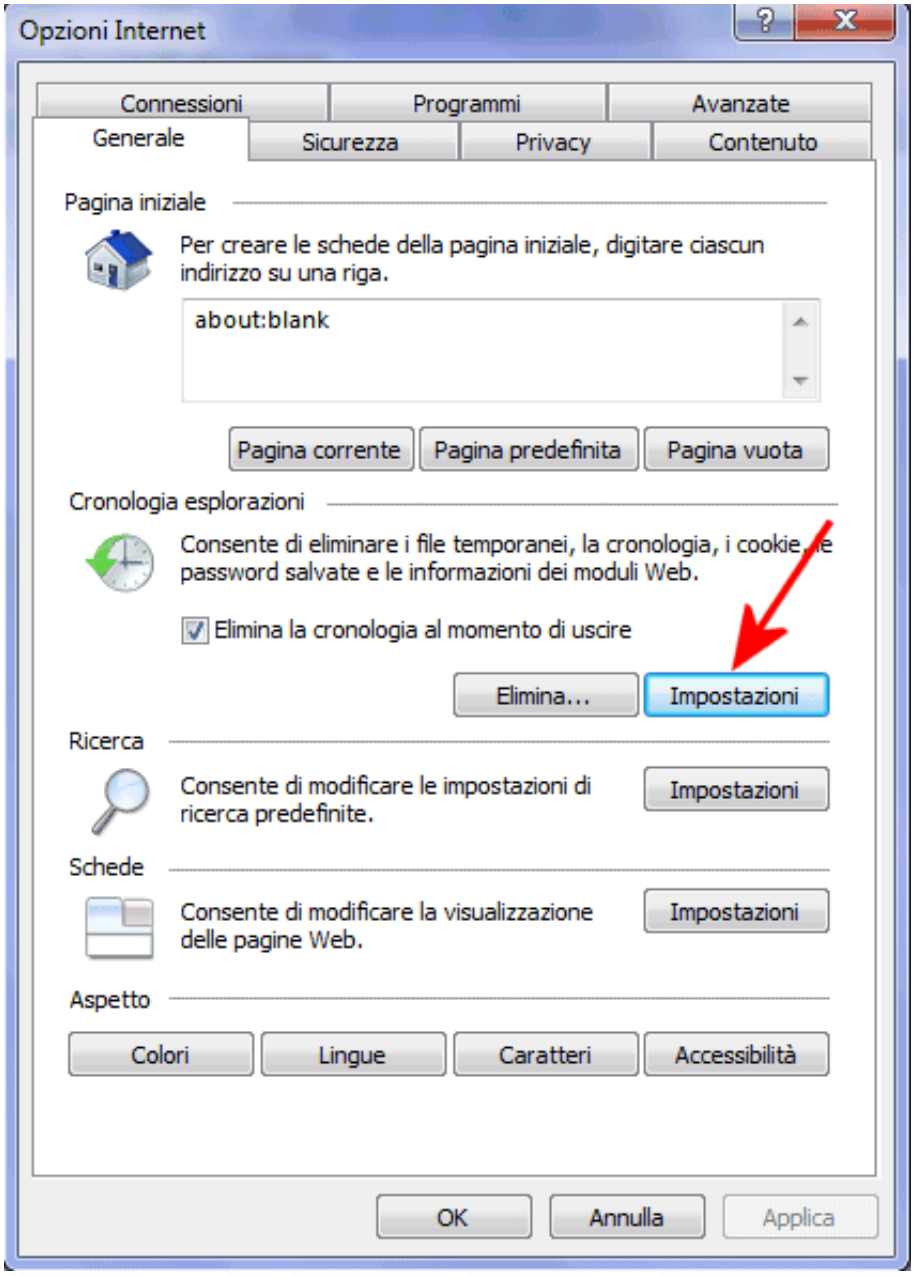


In corrispondenza della voce *Cancella i seguenti elementi da*, si dovrà selezionare *tutto*.

Per rimuovere i cookie dalle più recenti versioni di Microsoft **Internet Explorer**, è necessario cliccare sul pulsante a forma di ingranaggio, in alto a destra, selezionando *Opzioni Internet*:

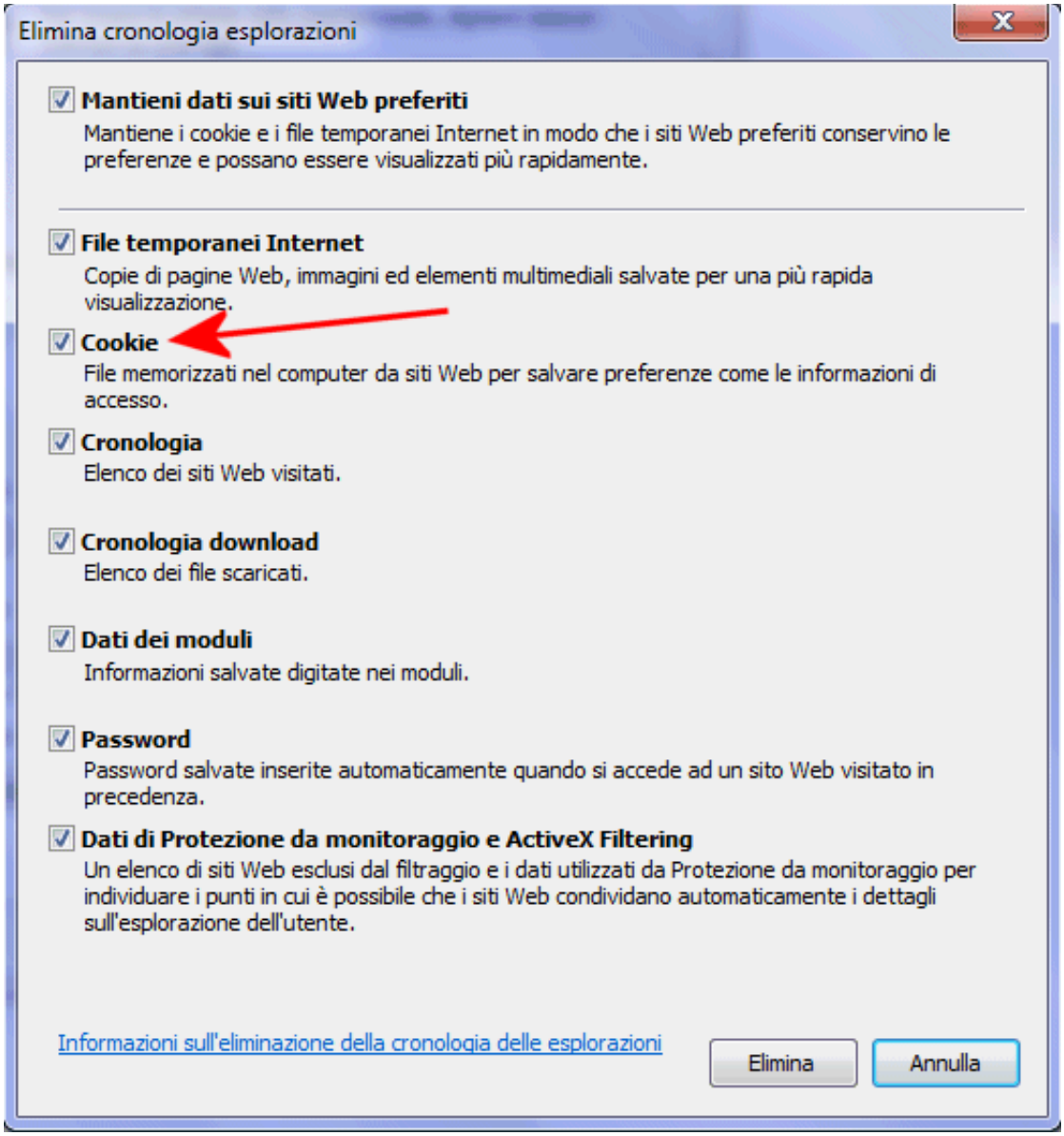


Dalla scheda *Generale*, si dovrà fare clic sul pulsante *Impostazioni* posta nella sezione *Cronologia esplorazioni*:



Alla comparsa della finestra *Impostazioni file temporanei Internet e cronologia*, si potrà cliccare su *Visualizza file*. Il risultato sarà l'apertura di una finestra di *Esplora risorse* contenente l'intera cache del browser. Scorrendo il contenuto della cartella, si noteranno dei file testuali la cui denominazione inizia con il prefisso cookie:. Sono proprio questi i cookie che il browser di Microsoft, di volta in volta, memorizza in locale.

Per **cancellare i cookie** completamente, il modo migliore consiste nel tornare alla finestra *Opzioni Internet* di Internet Explorer, fare clic sul pulsante *Elimina...* in corrispondenza di *Cronologia esplorazioni*, assicurarsi che la casella *Cookie* sia attiva e cliccare su *Elimina*:



La procedura da seguire nel caso di Apple Safari e di Opera è più o meno simile a quella vista nel caso di Firefox e Chrome.

Che cosa sono i cookie: la verità su come gestirli, rimuoverli e difendere la privacy sul web

I cookie contengono una serie di "proprietà" che permettono al browser web di "capire" quale server (sito web) li ha prodotti. L'attributo *domain* (dominio) comunica al browser a quale sito Internet deve essere restituito il contenuto del cookie mentre l'attributo *path* (percorso) indica quali *subdirectory* (sottocartelle) del dominio specificato sono da ritenersi valide.
Se, all'interno di un cookie è specificato come dominio, ad esempio, miodominio.it e come path /utenti, il contenuto del cookie sarà successivamente restituito solo alle pagine presenti su host come www.miodominio.it o ftp.miodominio.it che siano contenute all'interno della sottocartella utenti.
Oltre all'indicazione relativa al dominio ed al percorso, i cookie contengono altri quattro attributi: un *nome/valore*, una *scadenza* (questo dato stabilisce il periodo in cui il cookie deve essere ritenuto valido), una *modalità di accesso* (viene sfruttata per rendere invisibile il cookie a JavaScript così come ad altri linguaggi lato client utilizzati nelle pagine web) e una proprietà *sicuro* (stabilisce se il cookie debba essere trasmesso usando il protocollo HTTPS).

È comunque bene tenere sempre a mente che i cookie non sono "programmi" (sono semplici file testuali) e non possono assolutamente raccogliere informazioni in modo autonomo. In particolare, i cookie non possono in alcun modo "rubare" informazioni su di voi, all'interno del vostro personal computer. Essi possono essere utilizzati esclusivamente per memorizzare dei dati si sono digitati, in qualche circostanza, all'interno di uno o più siti web.
Per fare un esempio di tipo "benigno", supponete di aver inserito in un modulo (form) presente su un particolare sito web, il vostro colore preferito. Il server del sito provvederà a creare sul vostro personal computer un cookie contenente il nome del vostro colore preferito: non appena vi collegherete allo stesso sito Internet, il server verificherà la presenza dello stesso cookie all'interno del vostro computer, recupererà di nuovo le informazioni relative al vostro colore preferito e, per esempio, imposterà lo sfondo delle proprie

pagine web con tale colore in modo da accontentarvi.

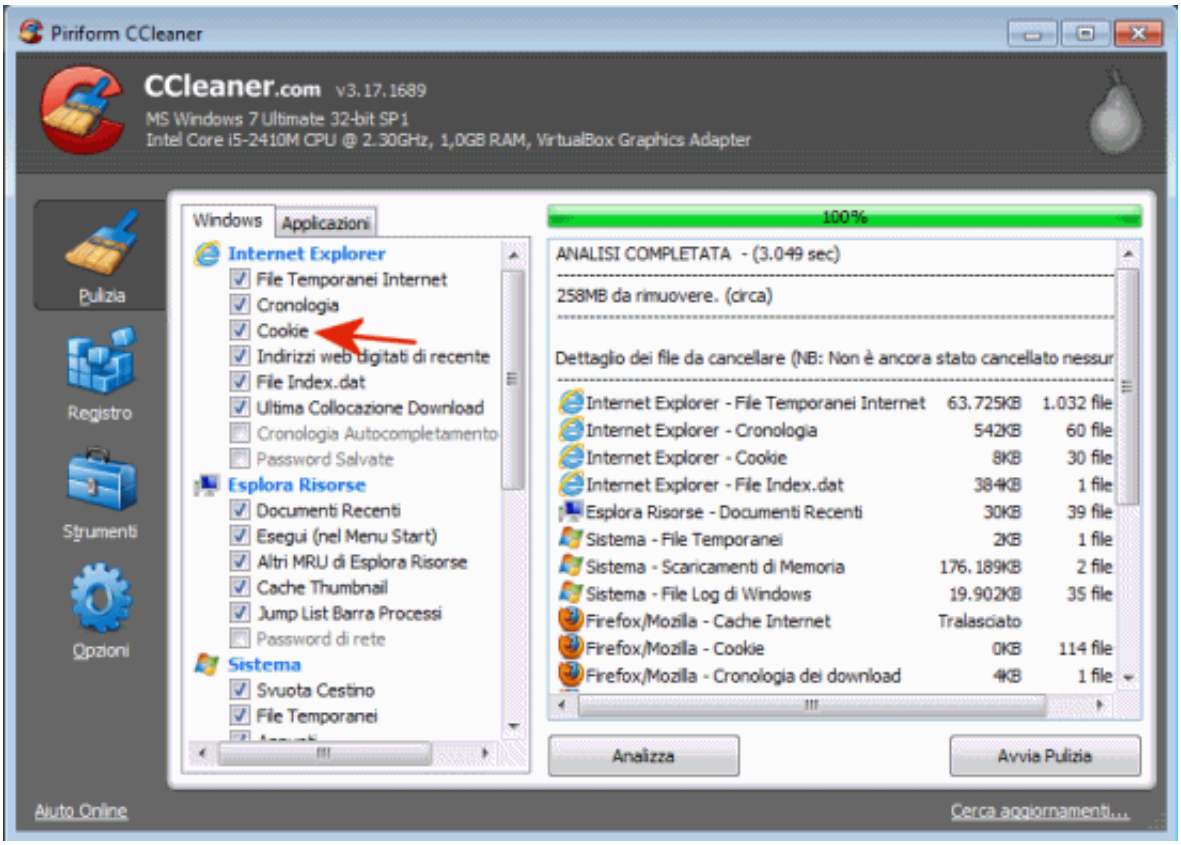
I cookie, come anticipato, possono essere comunque utilizzati con scopi meno "nobili". Ogni accesso ad uno specifico sito Internet lascia, grazie all'utilizzo dei cookie, informazioni sul vostro passaggio. Alcune società pubblicitarie hanno creato dei sistemi, basati sull'utilizzo di cookie, per effettuare una "profilazione" dettagliata degli utenti che "navigano" in Rete. I cookie, creati secondo specifiche standard, vengono distribuiti tra i vari siti web costituenti il network pubblicitario. In questo modo ogni volta che lo stesso utente visita uno dei siti web appartenenti al network, gli vengono proposti esclusivamente banner pubblicitari che possono potenzialmente essere più vicini ai suoi interessi.
Dal punto di vista grafico, i banner pubblicitari che compaiono sui siti web che utilizzano il sistema dei cookie, sono esattamente uguali a tutti gli altri. In realtà esiste una importante quanto, "ad occhio nudo", invisibile differenza... Quando un utente si connette per la prima volta al server pubblicitario (ciò avviene non appena egli visita un sito web che fa uso dei cookie per la gestione dei banner pubblicitari...), questo crea sul suo computer un cookie, all'interno del quale viene memorizzato un numero identificativo. Dopo un certo periodo di tempo, il server pubblicitario stila un elenco di tutti i siti web - facenti parte del network pubblicitario - che quello stesso utente ha visitato utilizzando così queste informazioni per creare un dettagliato profilo dell'utente con lo scopo di proporgli, successivamente, banner che possano attrarre maggiormente la sua attenzione.

Solitamente nomi e cognomi e/o indirizzi e-mail non fanno parte delle informazioni che le aziende pubblicitarie che fanno uso di questi sistemi gestiscono, tuttavia, altre informazioni che il browser fornisce (combinate con altri dati relativi a precedenti attività di uno stesso individuo), possono essere sufficienti per identificare uno stesso utente.

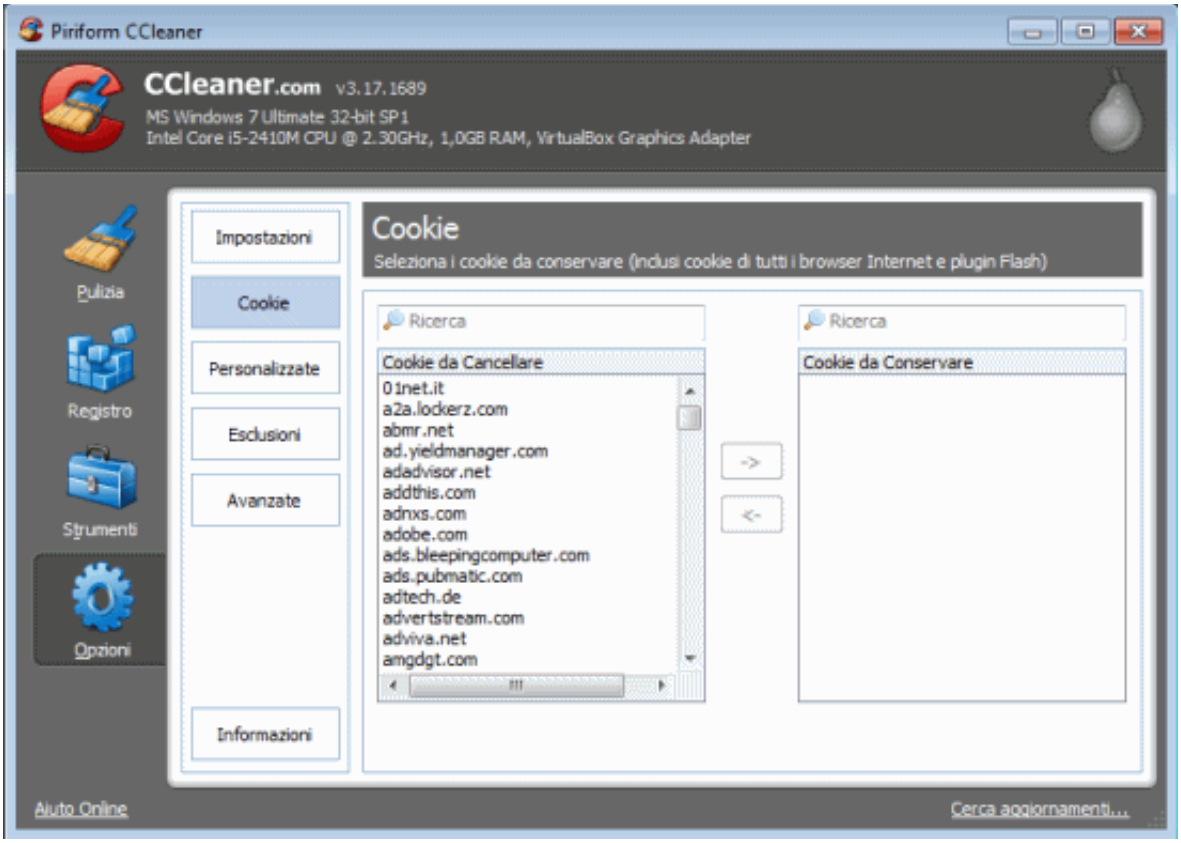
Uno dei consigli più utili è consiste quindi nel ripulire periodicamente la ca-

che del browser cancellando anche i cookie. Ovviamente si dovrà aver cura di non eliminare quelli più importanti; in caso contrario, si perderà il login sui principali siti che si frequentano con maggior interesse e frequenza.

Un software che consente di rimuovere i cookie (insieme con la cache ed altri elementi) da qualunque browser è il famoso **CCleaner**, prelevabile da questa scheda. Gratuito ed interamente in lingua italiana, CCleaner consente di sbarazzarsi di una vasta mole di informazioni superflue eventualmente conservate sul sistema in uso.
Per procedere con l'eliminazione dei cookie, basterà spuntare la casella *Cookie* dalla finestra principale, cliccare sul pulsante *Analizza* quindi su *Avvia pulizia*:



Cliccando su *Opzioni* poi su *Cookie* è eventualmente possibile definire un elenco di cookie da conservare e quindi non sottoporre mai ad eliminazione:



Ad ogni modo, a parte la comodità di continuare a restare loggati anche durante le successive sessioni di lavoro, proprio grazie ai cookie, alcuni esperti nel campo della sicurezza informatica continuano a ripetere, tutt'oggi, che l'effettuazione dell'operazione di logout è preferibile, soprattutto quando si visitano siti poco fidati. *Open Web Application Security Project* (OWASP), fondazione senza scopo di lucro che incentra le sue attività sulla produzione di risorse, articoli e materiale relativo a problematiche collegate con la sicurezza informatica, ha più volte posto l'accento sugli attacchi *Cross Site Request Forgery* (CSRF).

Si tratta di aggressioni che si concretizzano inviando ad un'applicazione web delle richieste sfruttando le autorizzazioni di un utente "*trusted*", ad esempio una persona che abbia effettuato il login su un determinato sito web.

Supponiamo che l'utente Bob sia loggato su un sito web di una banca e che, non effettuando il login, egli acceda - ad esempio - ad una pagina web dove il malintenzionato Mallory ha pubblicato un messaggio. Il messaggio preparato da Mallory contiene, ad esempio, una tag html IMG che fa riferimento ad uno script residente sul server della banca di Bob. Visitando la pagina "malevola", Bob potrebbe quindi inconsapevolmente dare il via ad un'opera-

zione che lui non ha richiesto.
Ecco perché è sempre consigliabile effettuare il logout da qualsiasi servizio online si stia utilizzando.
Un esempio su tutti? In passato una vulnerabilità CSRF fu scoperta dal ricercatore Petko D. Petkov, all'interno del servizio Google Gmail. In alcune schermate dimostrative pubblicate sul suo sito personale, Petkov illustrò una possibile forma di attacco: "*nell'esempio, l'aggressore prepara un filtro aggiuntivo che permette di estrarre le e-mail con allegato e le inoltra ad un altro indirizzo e-mail di sua scelta*", dichiarò il ricercatore. Un attacco potrebbe innescarsi nel momento in cui l'utente dovesse trovarsi a visitare un sito web maligno, opportunamente sviluppato per far leva sulla lacuna di sicurezza, rimanendo loggato al servizio GMail. Il problema fu prontamente risolto dai tecnici di Google e non ci risulta che un analogo incidente si sia riproposto ma l'esperienza suggerisce di agire con cautela anche in futuro.

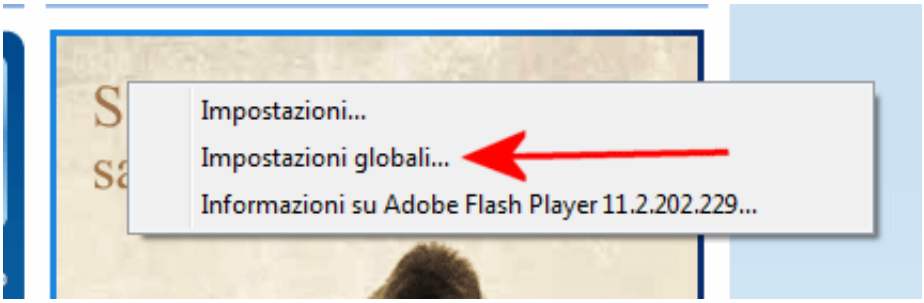
Che cosa sono i cookie: la verità su come gestirli, rimuoverli e difendere la privacy sul web

Se molto noti sono i cookie di tipo tradizionale, meno lo sono i cosiddetti **Flash cookie.** Rispetto ai classici cookie HTTP, i Flash cookie possono gestire un notevole quantitativo di dati: si passa dai 4 KB dei primi ai 100 KB dei secondi. I Flash cookie, poi, non hanno una data di scadenza impostata di default (abbiamo precedentemente conosciuto l'attributo "*scadenza*" nel caso dei normali cookie) e sono memorizzati in più locazioni sulla medesima macchina: anche andando alla ricerca dei file con estensione .SOL (questa l'estensione che contraddistingue i cookie Flash), è piuttosto difficoltoso individuarli velocemente.
Le impostazioni di sicurezza, inoltre, scelte a livello browser non hanno poi alcun effetto sui Flash cookie. Accedendo alle impostazioni avanzate di ciascun browser web è infatti possibile bloccare la ricezione dei cookie di tipo tradizionale o definire solo quei siti web che sono autorizzati a farne uso.
Se il browser può utilizzare il comunissimo plugin **Flash Player**, tutti i vari siti web che si visitano hanno modo di ricorrere a dei contenuti in formato Flash, esposti nelle pagine HTML, per provocare la memorizzazione di alcune informazioni sui sistemi client dei visitatori.
Ma com'è possibile verificare l'elenco dei siti web che hanno richiesto la memorizzazione di un Flash cookie sulla propria macchina? E com'è possibile controllare questo comportamento?

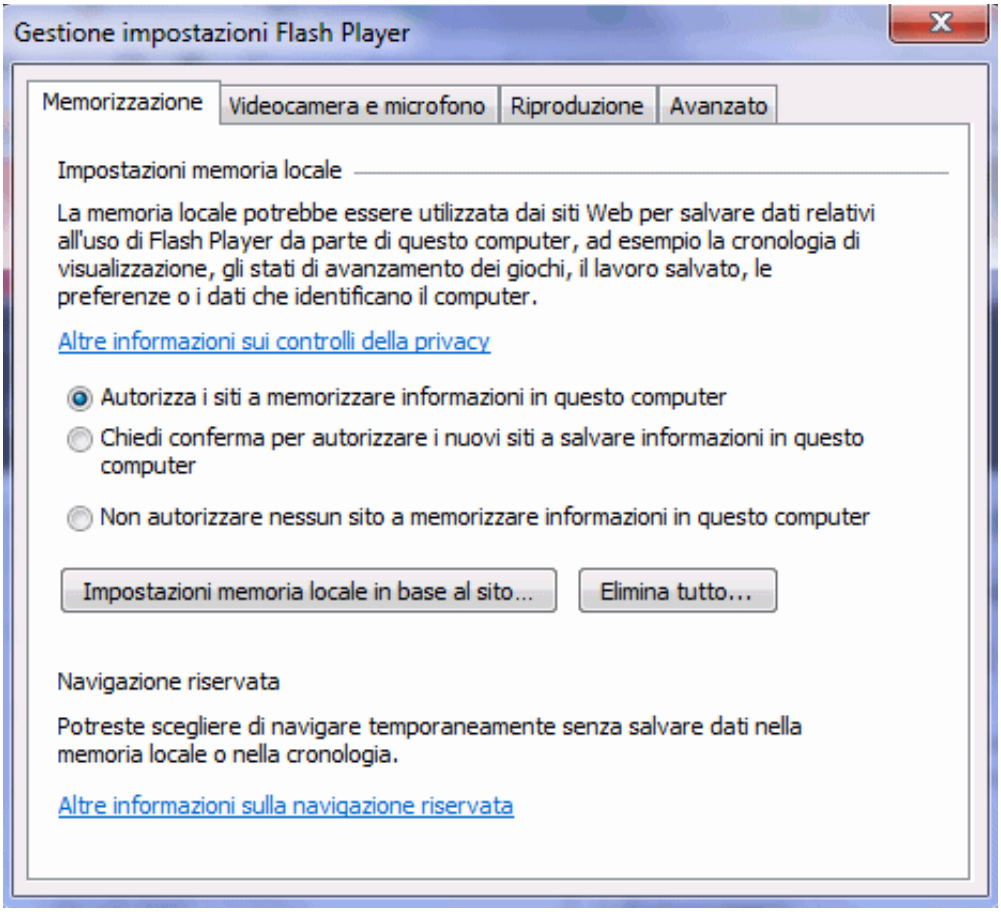
Se fino a qualche tempo fa Adobe non forniva uno strumento immediato (ad esempio, una utility "stand alone") per personalizzare le impostazioni di Flash Player connesse alla gestione dei cookie Flash, fortunatamente la situazione è stata sanata (peraltro in tempi piuttosto recenti).
Con il rilascio di **Flash Player 10.1** (giugno 2010), infatti, è stata aggiunta un'importante novità: utilizzando le funzionalità per la navigazione privata o "in incognito" integrate nei vari browser web (Internet Explorer, Firefox, Chrome, Safari ed Opera), Flash Player non memorizzerà i cookie Flash sul

sistema ma provvederà a rimuoverli alla chiusura della sessione di lavoro (ved., a tal proposito, questa pagina).
L'intervento di Adobe è la risposta alle eccezioni sollevate dalla *Federal Trade Commission* statunitense che aveva evidenziato alcune modalità di utilizzo poco trasparente, in alcuni siti web, dei Flash cookie. I commenti di Adobe sull'argomento sono raccolti in questo documento PDF.

Non solo. Se prima era obbligatoriamente necessario collegarsi con una scomoda pagina web ospitata sui server di Adobe per verificare l'elenco dei cookie Flash conservati sul proprio sistema, oggi è sufficiente fare clic con il tasto destro del mouse su un qualunque contenuto Flash esposto nelle pagine web e selezionare l'opzione *Impostazioni globali*:



Apparirà la seguente schermata:

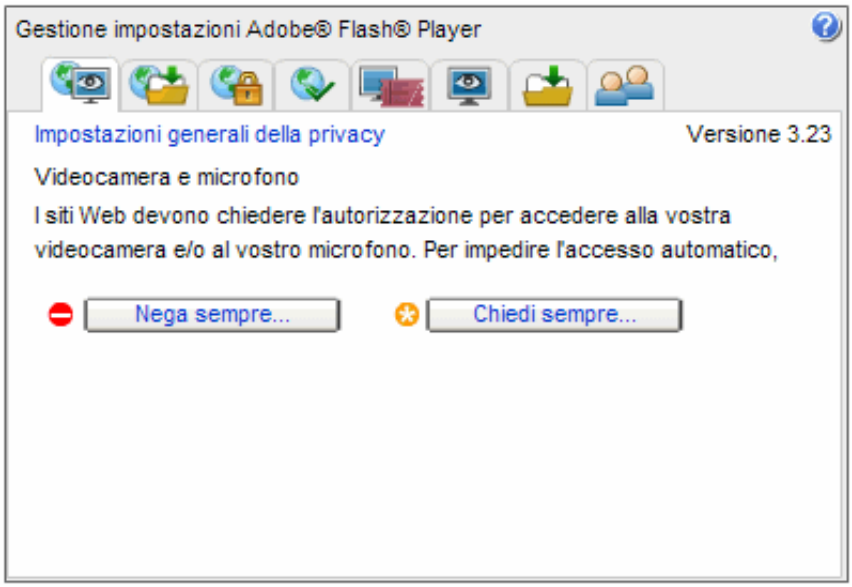


Come si vede, per impostazione predefinita, viene concessa a tutti i siti web l'autorizzazione per la memorizzazione di informazioni nel contesto locale ossia sul personal computer dell'utente attraverso l'uso dei Flash cookie (opzione *Autorizza i siti a memorizzare informazioni in questo computer*). Facendo clic sul pulsante *Impostazione memoria locale in base al sito*, si può controllare quali domini hanno usato i Flash cookie ed utilizzando il pulsante *Rimuovi* si potrà procedere con l'eliminazione dei vari elementi.

In alternativa, è possibile puntare il browser a questo indirizzo. Come spiega Adobe, il pannello di controllo visualizzato nella pagina del sito ufficiale della società non è un'immagine bensì è lo strumento che consente di personalizzare il comportamento di Flash Player.

Facendo riferimento alla sezione *Impostazioni generali della privacy*, si può evitare che qualunque sito web possa accedere al microfono od alla videocamera connessi al personal computer od anche solamente che possa richiederne

l'utilizzo.



Per controllare quali siti web hanno piazzato dei Flash cookie sul sistema, è sufficiente cliccare sulla linguetta "*Impostazione della memorizzazione dei siti web*" (la penultima scheda, da sinistra verso destra). In corrispondenza di ciascun sito web visitato, viene riportato il quantitativo di spazio che è stato impiegato per la memorizzazione di Flash cookie.
Agendo sui pulsanti *Elimina sito web* ed *Elimina tutto* si possono cancellare, rispettivamente, i Flash cookie creati dal sito evidenziato oppure tutti i Flash cookie.
Se si vuole evitare che i Flash cookie vengano memorizzati sul proprio sistema, è possibile accedere alla sezione *Impostazioni generali della memorizzazione* (seconda scheda da sinistra verso destra) e togliere il segno di spunta dalla voce *Consenti a contenuto Flash di terze parti di memorizzare dati sul computer*.

E' bene ricordare che se si eliminano i Flash cookie o se ne si disattiva completamente la memorizzazione, alcuni siti web potrebbero non operare più nel modo atteso. Si potranno certamente continuare a visualizzare file video distribuiti sul web attraverso l'uso della tecnologia Flash ma, ad esempio, si perderanno le informazioni relative, ad esempio, agli "scores" ottenuti con il proprio videogioco Flash preferito.

L'uso dei Flash cookie viene effettuato solitamente in modo "benigno". Tuttavia, come evidenziò già a suo tempo Bruce Schneier, i Flash cookie possono essere impiegati, ad esempio, per forzare una nuova creazione di un cookie HTTP tradizionale contenente le informazioni che esso ospitava precedentemente. Ciò diventa possibile grazie all'utilizzo delle informazioni "di backup" contenute all'interno del cookie Flash.

Che cosa sono i cookie: la verità su come gestirli, rimuoverli e difendere la privacy sul web

L'utilizzo ben poco rispettoso dei cookie Flash "profetizzato" da Bruce Schneier è di recente divenuto più comune con la nascita dei cosiddetti "*evercookie*". L'appellativo è stato scelto per descrivere l'abilità di questa particolare tipologia di cookie nel continuare ad essere "operativi" ed "utilizzabili" anche qualora l'utente dovesse richiederne l'eliminazione.
Rispetto ai cookie di tipo tradizionale ed ai cookie Flash di per sé, gli "*evercookie*" possono essere considerati una vera e propria minaccia per la privacy degli utenti anche sulla base dell'obiettivo primario a cui guardano: impedire la loro rimozione dai sistemi client.

Più che come un singolo cookie, l'"*evercookie*" può essere pensato come un meccanismo studiato per individuare in modo univoco un utente facendo leva sull'impiego di molteplici tecniche differenti (Flash cookie e vari sistemi per la memorizzazione dei dati utilizzando le specifiche HTML5).

Il merito di aver portato la pubblica attenzione su un tema delicato come quello degli "*evercookie*" spetta a Samy Kamkar, un ricercatore conosciuto per aver sviluppato un worm per MySpace nel 2005. Kamkar ha spiegato di aver messo a punto il suo esempio di "*evercookie*" nel giro di poche ore con l'intento di stimolare gli utenti a riflettere sulle nuove problematiche che il web e la complessità delle tecnologie oggi utilizzate portano con sé, soprattutto in materia di privacy.

Kamkar ha addirittura realizzato un'API JavaScript capace di automatizzare e semplificare la generazione di un "*evercookie*".

Diversamente rispetto ad un cookie tradizionale, che può essere agevolmente rimosso agendo, per esempio, sulle impostazioni del browser il cookie immortale "*evercookie*" è molto più difficoltoso da eliminarsi e mette in campo

diversi espedienti per rendere più complicata la sua completa rimozione. Sì, perché come i tentacoli di un mostro mitologico, anche l'*evercookie* è in grado di autorigenerarsi se almeno uno dei suoi componenti resta memorizzato sul sistema client dell'utente.

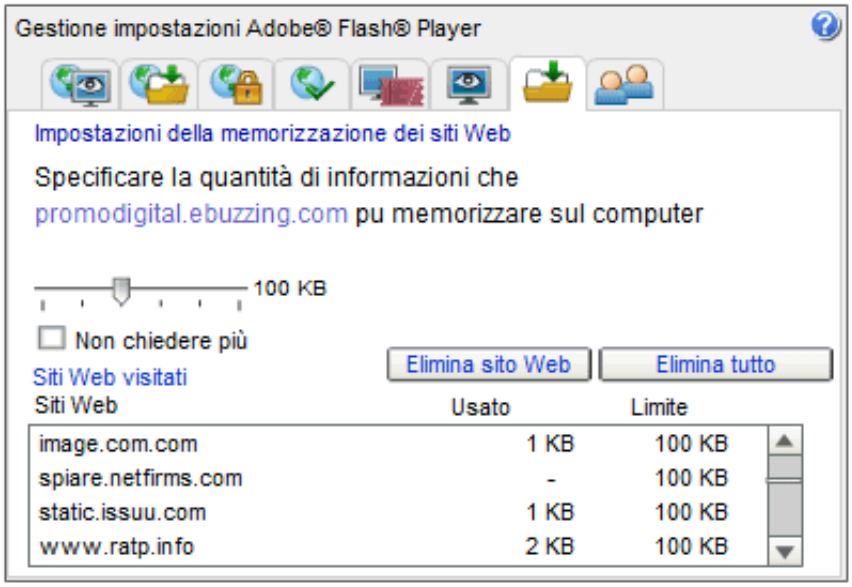
Il codice JavaScript messo a punto da Kamkar riesce a scrivere in diverse locazioni di memoria, utilizzando simultaneamente numerose tecniche. Se uno o più dati vengono cancellati, le informazioni che permettono di risalire in modo univoco al medesimo utente vengono recuperati attingendo alle risorse ancora disponibili sul sistema client. In particolare, l'API di Kamkar si appoggia, per la memorizzazione di un identificativo in grado di riconoscere l'utente, non solo ai *Flash cookies* ed ai cookie Silverlight, ma anche a tecniche quali "*PNG caching*" ed "*history caching*". Nel primo caso, l'identificativo viene stivato in un file PNG creato appositamente e che alcuni browser sono in grado di leggere usando l'elemento "canvas" di HTML5.
Con l'"history caching", invece, quando la pagina viene visitata per la prima volta ricorrendo al browser, il sito web codifica l'identificativo in un URL richiamato poi in background. Lo stesso identificativo può essere ricostruito a partire dalla cronologia del browser durante le visite seguenti.
È altamente improbabile che un utente con competenze medie riesca a cancellare ogni volta tutte le componenti alle quale attinge l'"*evercookie*": così, lasciando sul sistema anche una di esse, lo stesso utente potrebbe essere riconosciuto ogniqualvolta dovesse visitare la stessa pagina web.
La semplice rimozione del contenuto della cache del browser (eliminazione dei file temporanei) e dei cookie non consente infatti di mettersi alle spalle l'"*evercookie*" che dovesse essere stato eventualmente generato sul proprio sistema.

La procedura per eliminare tutte le componenti di un "evercookie"

1. Per cancellare definitivamente l'"*evercookie*", la procedura consigliata consiste, innanzi tutto, nel cancellare i cookie Flash seguendo la proce-

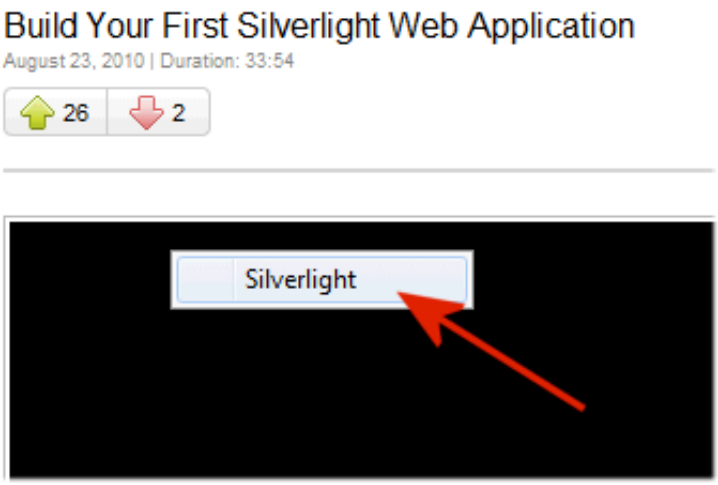
dura precedentemente illustrata. Se si preferisce usare il sito web di Adobe, basta collegarsi con questa pagina e cliccare sul pulsante "*Elimina tutto*" (è eventualmente possibile rimuovere i singoli cookie Flash selezionadoli quindi scegliendo "*Elimina sito web*").

Pannello Impostazioni della memorizzazione dei siti Web

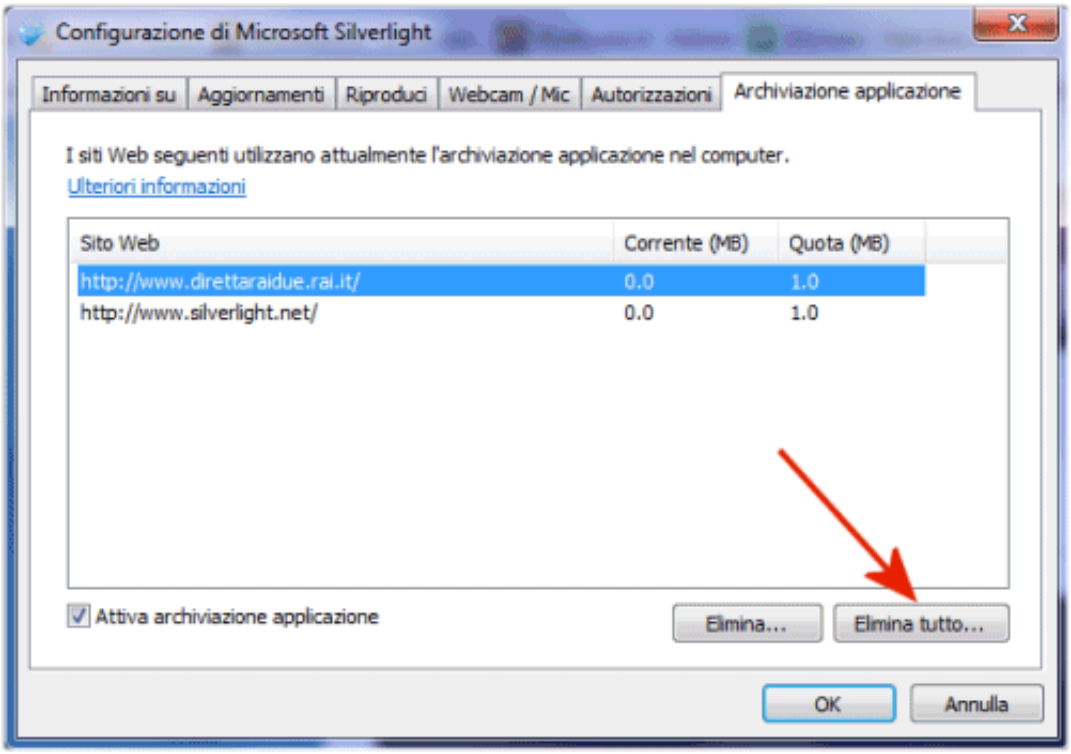


Ovviamente la procedura va eseguita solamente se sul browser in uso è stato installato il plugin Flash Player. La pagina web consente di eliminare rapidamente i Flash cookie senza dover visitare la cartella nella quale sono memorizzati (solitamente, %appdata%\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\ in Windows).

Qualora si fosse installato il pacchetto Microsoft **Silverlight** e quindi il browser web potesse caricare componenti realizzati utilizzando tale tecnologia, è necessario accedere a questo sito web, quindi visualizzare una qualunque cratività Silverlight. Suggeriamo, per esempio, di collegarvi con questa pagina, cliccare con il tasto destro del mouse sul video visualizzato all'interno della pagina e scegliere la voce *Silverlight*.



A questo punto per eliminare tutti i cookie Silverlight, è sufficiente selezionare la scheda *Archiviazione applicazione* quindi cliccare sul pulsante "*Elimina tutto*" premendo infine *Sì*.



È bene ricordare che se si agisce sui pulsanti "*Elimina tutto*", sia nel caso di Flash che nel caso di Silverlight, alcuni siti web potrebbero non operare più nel modo atteso. Si potranno certamente continuare a visualizzare file video distribuiti sul web attraverso l'uso della tecnologia Flash o Silverlight ma, ad esempio, si perderanno le informazioni relative, ad esempio, agli "*scores*" ot-

tenuti con il proprio videogioco preferito.

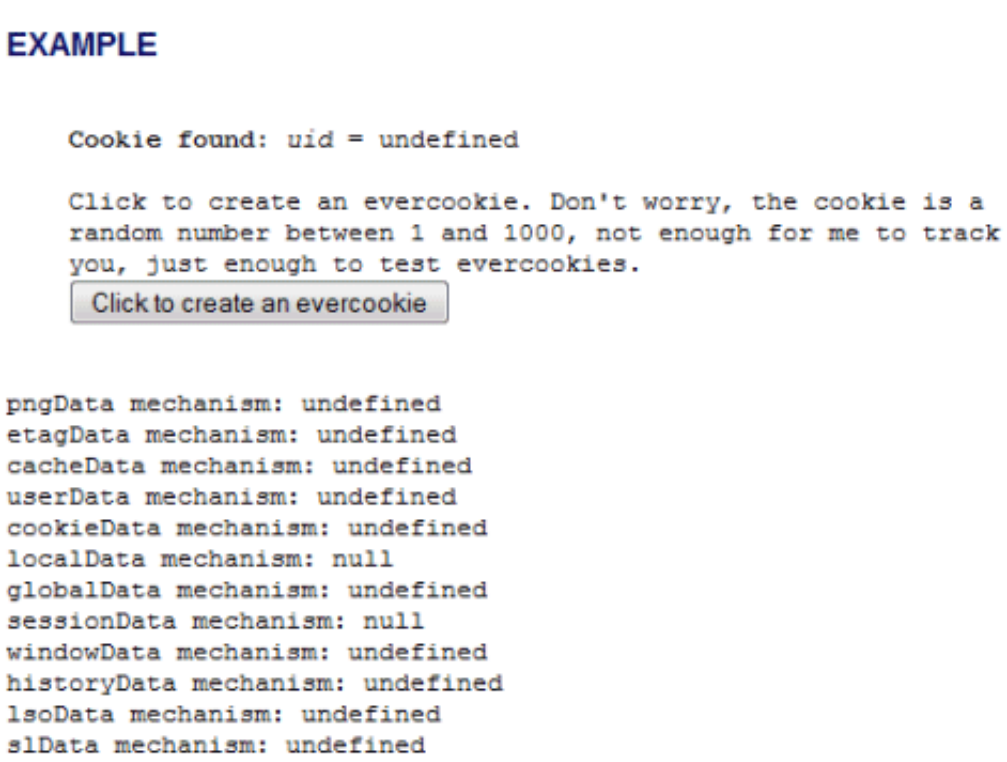

Come ultimo passo, è indispensabile accedere alla finestra per la cancellazione dei file temporanei del browser e rimuovere tutto il contenuto della cache (cookie tradizionali compresi).


A questo punto è indispensabile chiudere e riaprire il browser web.

Samy Kamkar ha messo a punto una pagina dimostrativa che consente all'utente di prendere coscienza del problema "*evercookie*".
Collegandosi con la pagina allestita dal ricercatore quindi cliccando sul pulsante *Click to create an evercookie*, la pagina web metterà in atto una serie di espedienti che porteranno alla generazione di un "*evercookie*" sul sistema dell'utente.

Ricaricando la medesima pagina, dopo qualche secondo di attesa, dovrebbe essere proposto un ID compreso tra 1 e 1000. Se si prova a cancellare la cache del browser, tornando sulla medesima pagina di test, verrà visualizzato - con buona probabilità - sempre il medesimo numero identificativo.
Nel caso in cui venisse visualizzato l'attributo "*undefined*", l'operazione compiuta (cancellazione della cache) è sufficiente per mettersi al riparo da eventuali siti traccianti dal momento che sul sistema non è presente né Flash Player né Microsoft Silverlight.

Seguendo i quattro passi sopra illustrati, sarà possibile cancellare definitivamente tutte le componenti dell'"*evercookie*" di test. In questo modo, riaprendo il browser web e tornando a visitare la pagina predisposta da Kamkar dovrebbe essere esposta l'indicazione "*undefinied*" accanto a ciascuna delle voci indicate.



La dizione "*Cookie found: uid = undefined*" conferma il fatto che il sistema client non è più "riconoscibile" in modo univoco.