Appendice tecnica – Analisi dei cookie HTTP (livello utente e forense)

Appendice agli articoli pubblicati sui seguenti canali:

• CLOG – corporate blog su esperti.com/blog: «Cookie HTTP: cosa sono, come funzionano e come analizzarli (anche in chiave forense)».

• PLOG – personal blog su giovannigrandesso.com/blog: «Cookie, banner e «accetta tutto»: anatomia di una finta scelta».

1. Scopo e campo di applicazione

Questa appendice definisce un protocollo tecnico dettagliato per l'analisi dei cookie HTTP generati da un sito web, pensato per due livelli di utilizzo:

• livello «utente evoluto»: lettori del CLOG/PLOG, legali, DPO, responsabili IT che vogliono verificare in autonomia cosa un sito scrive nel browser;

• livello «forense»: consulenti tecnici che devono produrre, in una perizia o in un audit, evidenze strutturate e ripetibili sull'uso o sulla mancata evidenza d'uso di cookie.

L'obiettivo è fornire una guida operativa sufficientemente granulare da poter essere citata come «protocollo di laboratorio» all'interno di una relazione, con esempi concreti di comandi, strutture dati e modelli di reportistica.

2. Definizione operativa di cookie HTTP

Per il presente documento, un cookie HTTP è una coppia nome=valore associata a uno specifico dominio e percorso, dotata di attributi opzionali (scadenza, flag di sicurezza), che il server invia al browser con l'intestazione di risposta Set-Cookie e che il browser reinvia automaticamente al server nelle richieste successive tramite l'intestazione Cookie.

Metafora di lavoro: il cookie è un badge di riconoscimento che la portineria (server) consegna al visitatore (browser). Il badge contiene un ID, una data di scadenza e regole d'uso (dove vale, quando può essere mostrato, chi può leggerlo). Ad ogni nuovo ingresso nello stesso edificio (nuova richiesta HTTP verso lo stesso dominio) il badge viene mostrato automaticamente, senza che l'utente debba ricordarsene.

3. Ruolo dei cookie nell'architettura HTTP

HTTP nasce come protocollo stateless: ogni richiesta è indipendente e il server non ha memoria delle precedenti. I cookie introducono uno strato di «memoria applicativa» che permette di legare tra loro più richieste provenienti dallo stesso browser. In pratica consentono di:

• mantenere sessioni di autenticazione (riconoscere che l'utente è già loggato);

• associare carrelli di acquisto, preferenze e impostazioni alle richieste successive;

• conteggiare i visitatori e ricostruire percorsi di navigazione sulla base di identificativi persistenti;

• tracciare nel tempo e su più siti il comportamento di un dispositivo, ai fini di profilazione e targeting pubblicitario.

4. Tassonomia dei cookie utile all'analisi

Per strutturare l’analisi è utile classificare i cookie secondo tre dimensioni: durata, provenienza, scopo.

4.1 Durata

• Cookie di sessione: nessun attributo Expires o Max-Age. Persistono solo per la durata della sessione; vengono eliminati alla chiusura del browser o della scheda.

• Cookie persistenti: dotati di Expires (data/ora assoluta) o Max-Age (seconds-to-live). Permettono di riconoscere il dispositivo anche a distanza di giorni, settimane o mesi.

Metafora: il cookie di sessione è il badge giornaliero che restituisci a fine turno; il persistente è la tessera fedeltà che tieni sempre nel portafoglio.

4.2 Provenienza (first-party / third-party)

• First-party: impostati dal dominio che compare nella barra degli indirizzi (es. www.esperti.com).

• Third-party: impostati da domini esterni integrati nella pagina (es. network pubblicitari, social, analytics di terze parti).

Metafora: un badge emesso direttamente dall’azienda in cui ti trovi (first-party) rispetto a un badge di una società esterna che però funziona in più aziende convenzionate (third-party).

4.3 Scopo (tecnici, analytics, profilazione)

• Tecnici: necessari a fornire il servizio richiesto (login, carrello, sicurezza, bilanciamento).

• Analytics: usati per misurare traffico, conversioni, funnel. Possono essere gestiti dal titolare o da terzi.

• Profilazione / marketing: costruiscono nel tempo uno storico dettagliato delle azioni associate a un identificativo.

In ambito forense è prudente descrivere tutti questi elementi in modo oggettivo (dominio, durata, pattern del valore) e collegarli, se necessario, alla documentazione del titolare; la qualificazione giuridica resta responsabilità del legale.

5. Attributi dei cookie: analisi tecnica ed esempi

5.1 Esempio di Set-Cookie

Esempio di intestazione Set-Cookie in una risposta HTTP:

```
Set-Cookie: PHPSESSID=1a2b3c4d5e6f7g8h9i; Path=/; HttpOnly; Secure; SameSite=Lax
```

In questo caso abbiamo:

• nome: PHPSESSID (cookie tipicamente usato da applicazioni PHP per la sessione);

• valore: 1a2b3c4d5e6f7g8h9i (identificativo di sessione opaco);

• Path=/ (valido per l’intero sito);

• HttpOnly (non leggibile da JavaScript);

• Secure (inviato solo su HTTPS);

• SameSite=Lax (inviato in un sottoinsieme di contesti cross-site).

5.2 Expires e Max-Age

Altro esempio:

```
Set-Cookie: _ga=GA1.2.123456789.987654321; Expires=Tue, 31 Dec 2030 23:59:59 GMT;
Path=/; Secure
```

Una scadenza così lontana nel tempo suggerisce un uso di lungo periodo (analytics o profilazione). In tabella andrà annotato come cookie persistente con data di scadenza specifica, evidenziando l’orizzonte temporale.

5.3 Domain, Path, Secure, HttpOnly, SameSite

La combinazione di Domain, Path, Secure, HttpOnly e SameSite definisce il perimetro tecnico di utilizzo del cookie. In un’ottica di audit si valuterà, ad esempio, se cookie di sessione critici sono limitati a HTTPS, se sono protetti da HttpOnly, se SameSite è impostato in modo coerente con la logica del sito.

6. Strumenti di analisi lato utente (DevTools)

Senza ricorrere a strumenti esterni è già possibile ottenere molto con gli strumenti di sviluppo del browser. Di seguito una procedura generica, esemplificata su Firefox ma adattabile ad altri browser moderni.

6.1 Network / Rete

1) Aprire il sito in una nuova finestra o in un profilo pulito.

2) Premere F12 per aprire gli Strumenti di sviluppo e selezionare il pannello «Rete» / «Network».

3) Abilitare la conservazione del log, se non attiva di default.

4) Caricare o ricaricare la pagina principale del sito.

5) Selezionare alcune richieste significative (es. il documento HTML principale, le chiamate a script di terze parti) e ispezionare le intestazioni di risposta per identificare eventuali Set-Cookie; nelle richieste successive, ispezionare le intestazioni di richiesta per vedere quali Cookie vengono inviati.

6.2 Storage / Archiviazione

1) Dal pannello degli strumenti di sviluppo selezionare «Archiviazione» / «Storage».

2) Espandere la sezione «Cookie» per vedere l’elenco dei domini per cui sono presenti cookie.

3) Selezionare il dominio principale del sito e i domini terzi più sospetti (ad esempio quelli che richiamano pagine di advertising o analytics).

4) Esaminare per ciascun cookie nome, valore, dominio, percorso, scadenza e attributi, annotando quelli più rilevanti per l’obiettivo d’indagine.

6.3 Console JavaScript

Nella console del browser è possibile digitare:

```
document.cookie
```

per ottenere la stringa di cookie accessibili a JavaScript nella pagina corrente. Questo elenco non include i cookie contrassegnati HttpOnly, ma può essere utile per vedere quali informazioni sono direttamente disponibili agli script client-side (ad esempio script di terze parti integrati nel sito).

6.4 Limiti dell’analisi a vista

L’uso dei DevTools è sufficiente per una prima diagnosi, ma non garantisce da solo la ripetibilità e l’integrità necessarie in ambito forense. Per questo si introduce una procedura strutturata con file HAR, database dei cookie e, se necessario, PCAP.

7. Preparazione dell’ambiente forense

Per acquisizioni a valore probatorio si raccomanda di utilizzare una macchina virtuale dedicata o almeno un profilo di browser separato, con le seguenti precauzioni:

• azzerare precedenti dati di navigazione (cronologia, cache, cookie);

• non installare estensioni che alterino il comportamento dei cookie (ad-blocker, privacy enhancer);

• documentare versione del browser, sistema operativo, data e ora (incluso fuso orario), configurazione di rete (presenza di proxy, VPN), eventuali snapshot della VM.

8. Procedura operativa forense estesa

8.1 Esempio di scenario di navigazione

A titolo di esempio, uno scenario di prova per un sito X potrebbe essere:

• T0: accesso alla homepage senza interagire con il banner dei cookie;

• T1: rifiuto dei cookie non tecnici (se il banner lo consente);

• T2: nuova visita con accettazione di tutti i cookie;

• T3: eventuale login con account di test;

• T4: navigazione di alcune pagine rilevanti (es. area riservata, carrello, sezione news).

8.2 HAR: esportazione e struttura rilevante

Una volta completato lo scenario, dal pannello Rete si esporta il log in formato HAR. Nel file risultante ogni voce contiene richieste e risposte con intestazioni. La parte di interesse per i cookie è tipicamente nel blocco response.headers (per Set-Cookie) e request.headers (per Cookie).

In relazione si possono riportare estratti testuali di tali intestazioni, indicando il nome del file HAR, la voce corrispondente (es. entry #12) e l'istante temporale.

8.3 Database locale dei cookie: posizione e query

Nel caso di Firefox su GNU/Linux, il file dei cookie è generalmente situato in:

```
~/.mozilla/firefox/<profilo>/cookies.sqlite
```

Dopo aver chiuso il browser è possibile copiare questo file in una cartella di reperti ed analizzarlo con sqlite3.

Esempio di comando per estrarre i cookie relativi a un dominio:

```
sqlite3 cookies.sqlite \ "SELECT host, name, value, expiry, isSecure, isHttpOnly,
sameSite FROM moz_cookies WHERE host LIKE '%esempio.com%' ORDER BY host, name;"
```

Il risultato, eventualmente esportato in CSV, costituisce una tabella facilmente allegabile alla perizia. L'analisi incrociata tra questo output e il file HAR permette di verificare che i cookie impostati dal server siano effettivamente presenti nello storage locale del browser.

9. Cattura di rete (PCAP) con tcpdump / Wireshark

La cattura di pacchetti di rete non è sempre necessaria, ma aggiunge un ulteriore livello di dettaglio. Esempio di comando tcpdump per catturare il traffico HTTP/HTTPS verso un determinato host:

```
sudo tcpdump -i eth0 -w sitoX.pcap host www.esempio.com
```

La cattura va attivata prima di avviare lo scenario di navigazione e terminata alla fine. Il file sitoX.pcap può essere aperto con Wireshark, applicando filtri del tipo:

```
http.cookie || http.set_cookie
```

per evidenziare solo i pacchetti che contengono intestazioni Cookie o Set-Cookie. Questo permette di verificare, a livello di pacchetto, lo stesso flusso evidenziato nel file HAR.

10. Correlazione delle evidenze e conclusioni (base)

La forza dell'analisi sta nella correlazione coerente di più sorgenti:

• HAR: mostra quando e come il server ha chiesto di impostare cookie e quando il browser li ha inviati;

• database locale: mostra quali cookie risultano effettivamente memorizzati nel profilo analizzato;

• PCAP (se presente): mostra le stesse intestazioni a livello di pacchetto, utile in contesti in cui si vuole escludere manipolazioni lato browser.

11. Caso di studio sintetico: analisi del sito «sitoX»

Per rendere più concreto il protocollo, si consideri un caso di studio fittizio su un sito denominato «sitoX» raggiungibile all'indirizzo www.sitox.example.

11.1 Scenario di prova

Lo scenario prevede due sessioni distinte, eseguite in profili puliti diversi:

• Sessione A: l'utente rifiuta tutti i cookie non tecnici dal banner;

• Sessione B: l'utente accetta tutti i cookie.

Per entrambe le sessioni vengono acquisiti file HAR, copie di cookies.sqlite e, facoltativamente, PCAP.

11.2 Estratto semplificato del file HAR

In Sessione B il file HAR contiene, tra le altre, la seguente intestazione di risposta per la risorsa HTML principale:

```
HTTP/2 200 OK\nContent-Type: text/html; charset=UTF-8\nSet-Cookie:
sitox_session=abc123xyz; Path=/; HttpOnly; Secure; SameSite=Lax\nSet-Cookie:
consent_marketing=1; Path=/; Expires=Tue, 31 Dec 2030 23:59:59 GMT;
Secure\nSet-Cookie: tracker_id=9f8e7d6c5b4a3; Domain=.adnetwork.example; Path=/;
Expires=Tue, 31 Dec 2030 23:59:59 GMT; Secure
```

Le richieste successive verso www.sitox.example e verso script di adnetwork.example mostrano intestazioni Cookie che includono questi identificativi. In Sessione A, invece, compaiono solo sitox_session e nessun cookie di consenso o di tracking.

11.3 Estratto da cookies.sqlite

L'estrazione dal database locale in Sessione B evidenzia, ad esempio:

```
host name value expiry isSecure isHttpOnly sameSite\n-------------------
---------------- ------------ ------------ -------- ----------
--------\nwww.sitox.example sitox_session abc123xyz 1735689599 1 1
1\nwww.sitox.example consent_marketing 1 1924991999 1 0 0\n.adnetwork.example
```

```
tracker_id 9f8e7d6c5b4a3 1924991999 1 0 0
```

I valori di expiry (in secondi Unix) corrispondono alla data di fine 2030, confermando la natura persistente dei cookie di consenso e tracking.

11.4 Sintesi tecnica del caso «sitoX»

Dalla correlazione tra HAR e cookies.sqlite si può concludere che:

• «sitoX» imposta sempre un cookie tecnico di sessione (sitox_session) con attributi Secure+HttpOnly+SameSite=Lax;

• a seguito dell'accettazione dei cookie, vengono impostati un cookie first-party di consenso (consent_marketing) e un cookie third-party di tracking (tracker_id) su adnetwork.example, entrambi persistenti con scadenza 2030;

• in Sessione A (rifiuto) non risultano impostati né consent_marketing né tracker_id.

Questi elementi possono essere riportati in perizia in forma tabellare, collegando per ciascun cookie le evidenze HAR, SQLite e (se presenti) PCAP.

12. Modello di tabella di reportistica (con esempio compilato)

Di seguito un modello di tabella da includere in perizia, accompagnato da una compilazione esemplificativa per il caso «sitoX».

Intestazioni suggerite:

• Nome cookie;

• Dominio (first-party / third-party);

• Scopo (tecnico / analytics / profilazione – se deducibile);

• Durata (sessione / persistente + data di scadenza);

• Attributi principali (Secure, HttpOnly, SameSite);

• Fonti di evidenza (file HAR, riga CSV, ID pacchetto PCAP);

• Note (osservazioni, collegamenti all'informativa del titolare, eventuali criticità).

Esempio parziale di riga compilata per «sitoX»:

```
Nome: sitox_session\nDominio: www.sitox.example (first-party)\nScopo: tecnico (sessione autenticazione)\nDurata: sessione (expiry coerente con chiusura browser)\nAttributi: Secure=1, HttpOnly=1, SameSite=Lax\nEvidenze: HAR (entry #12, Set-Cookie), cookies.sqlite (riga 1 dell'estrazione), sitoX.pcap (pacchetti con http.set_cookie)\nNote: cookie necessario al funzionamento del servizio, non utilizzato per profilazione.
```

Per consent_marketing e tracker_id le righe conterranno invece durata pluriennale, scopo orientato alla profilazione e riferimenti a domini terzi per il cookie di tracking, con possibili criticità rispetto alle dichiarazioni del titolare del sito.

13. Oltre i cookie: Web Storage e fingerprinting

I cookie sono solo una delle tecnologie di persistenza e tracciamento disponibili. Le Web Storage API consentono di memorizzare dati nel browser in strutture come localStorage e sessionStorage; IndexedDB permette storage più complesso; tecniche di device fingerprinting possono «riconoscere» un dispositivo anche senza cookie persistenti, combinando informazioni sul browser e sull'hardware.

In un audit completo conviene quindi estendere l'analisi oltre i soli cookie, soprattutto nei casi in cui il sito dichiara di non utilizzarli ma mostra comunque pattern sospetti di tracciamento.

14. Catena di custodia e integrità dei reperti

Affinché i file HAR, cookies.sqlite e PCAP possano essere presi sul serio in un contesto contenzioso è opportuno curare anche alcuni aspetti di catena di custodia e integrità:

• assegnare a ciascun reperto un nome univoco che includa data, ora e identificativo del caso (es. CTP-1234_sitoX_2025-12-04T1030Z.har);

• calcolare e registrare hash crittografici (es. SHA-256) dei file immediatamente dopo l'acquisizione, annotandoli nella relazione o in un verbale separato;

• conservare i file in un'area protetta, con backup adeguato e controllo degli accessi;

• documentare chi ha effettuato l'acquisizione, con quali strumenti, in quali condizioni operative (macchina fisica/virtuale, versioni software).

Questi accorgimenti non fanno parte stretta dell'analisi dei cookie, ma contribuiscono a rendere la metodologia credibile e difficilmente attaccabile sotto il profilo procedurale.

15. Linee guida per l’uso dell’appendice in perizie e altri elaborati

L’appendice può essere richiamata in perizie, note tecniche, pareri pro veritate e documenti di audit in vari modi, ad esempio:

• «L’analisi è stata condotta seguendo il protocollo operativo descritto in “Appendice tecnica – Analisi dei cookie HTTP (livello utente e forense)”, allegata agli articoli CLOG (esperti.com/blog – corporate blog) e PLOG (giovannigrandesso.com/blog – personal blog).»

• «Per la definizione delle categorie di cookie e la procedura di raccolta delle evidenze (HAR, database locale, PCAP) si fa rinvio al documento di riferimento sopra citato, salvo gli adattamenti descritti nel presente elaborato.»

L’idea è evitare di riscrivere ogni volta l’intero protocollo, potendo invece richiamarlo come standard de facto, aggiornabile nel tempo.

16. Limiti del presente documento e aggiornabilità

Questo documento riflette lo stato dell’arte dei browser, dei meccanismi di cookie e delle pratiche forensi al momento della sua redazione (dicembre 2025). Evoluzioni future dei browser (in particolare nelle politiche di gestione delle terze parti e nel blocking by default) potrebbero richiedere aggiornamenti della procedura.

È consigliabile, in caso di utilizzo in procedimenti o progetti di medio-lungo periodo, verificare periodicamente la coerenza delle indicazioni qui contenute con la documentazione ufficiale dei browser e degli strumenti utilizzati.

17. Collegamento con CLOG (esperti.com/blog) e PLOG (giovannigrandesso.com/blog)

Questa appendice è progettata per essere allegata agli articoli del corporate blog CLOG su esperti.com/blog e del personal blog PLOG su giovannigrandesso.com/blog. Nel CLOG fornisce la base tecnica a supporto di quanto esposto in forma divulgativa; nel PLOG offre al lettore interessato gli strumenti per andare oltre la critica ai banner «accetta tutto» e verificare in prima persona cosa il browser sta realmente facendo.

In contesti professionali (perizie, audit, attività di consulenza) può essere citata come «Appendice tecnica – Analisi dei cookie HTTP (livello utente e forense)», adattando all’occorrenza lo scenario di navigazione e gli strumenti utilizzati, ma mantenendo invariati i principi di ripetibilità, documentazione e chiarezza metodologica.