IISFA
ASSOCIAZIONE ITALIANA
DIGITAL FORENSICS

5 maggio 2020

Acquisizione della Prova online

Paolo Dal Checco, *Consulente Informatico Forense*
www.dalchecco.it

Linee guida e normative di DF e IR

- RFC 2350: "Expectations for Computer Security Incident Response"
- RFC 3225: *"Guidelines for Evidence Collection and Archiving"*
- ISO 27035: *"Information security incident management"*
- ISO 27037: ***"Guidelines for identification, collection, acquisition and preservation of digital evidence"***
- *ISO 27041: Guidance on assuring suitability and adequacy of incident investigation methods*
- *ISO 27042: Guidelines for the analysis and interpretation of digital evidence*
- *ISO 27043: Incident investigation principles and processes*

Le fasi dell'Informatica Forense

- Il processo di investigazione forense prevede le seguenti fasi:
  - Identificazione
  - Preservazione
  - Acquisizione
  - Analisi
  - Presentazione dei risultati

Identificazione

- Una volta identificato cosa acquisire bisogna:
- Saper valutare cosa va acquisito e cosa è trascurabile
- Essere in grado di acquisire tutto quello che è necessario
- "Etichettare" univocamente ogni supporto
- Assegnare un identificativo associato alla descrizione (marca, modello, seriale, ubicazione, stato ecc.)
- Stabilire il piano di acquisizione efficace

Acquisizione

- Bisogna rispettare un ordine di volatilità:
  - Registri, cache
  - Memorie RAM
  - Stato della rete (connessioni stabilite, socket in ascolto, applicazioni coinvolte, cache ARP, routing table, DNS cache ecc.)
  - Processi attivi
  - Memorie di massa (hard disk, pendrive USB, ecc.)
  - Log remoti
  - Floppy, nastri e altri dispositivi di backup
  - Supporti ottici
- Le copie eseguite devono essere identiche all'originale (integrità e non ripudiabilità) → **calcolo valori hash**
- Le procedure devono essere documentate e attuate secondo metodi e tecnologie conosciute, così da essere verificabili dalla controparte

Preservazione

- Spesso questa "fase" viene omessa e inglobata in altre
- Non bisogna alterare il reperto originale (Write blocker / Distribuzione Forense)
- Se inevitabile, alterare il meno possibile e documentare

Analisi

- Estrarre i dati e processarli per ricostruire informazioni
- Interpretare le informazioni per individuare elementi utili alle indagini
- Comprendere e correlare, in modo da affinare le ricerche e poterne trarre le conclusioni
- E' sicuramente la fase più laboriosa di tutto il processo e richiede conoscenze disparate

Presentazione

- Alla fine dell'attività di analisi, si deve presentare quanto elaborato, in una relazione tecnica:
- I risultati devono essere presentati in forma facilmente comprensibile a tutti
- I destinatari non hanno di solito competenze informatiche approfondite
- E' probabile che la relazione venga esaminata da un tecnico di parte
- Essere semplici e chiari, non bisogna essere superficiali e approssimati

Tipologie di dati online

- Siti web, forum, gruppi di discussione
- Profili, pagine, gruppi su Facebook, Linkedin o Twitter
- File sharing
- Streaming (es. Youtube)
- Servizi o applicazioni desktop o mobile (es. Tripadvisor, Google Earth, etc…)
- Chat, gruppi, supergruppi, canali e bot Telegram
- Messaggi Facebook Messenger, Whatsapp, Twitter, Linkedin, etc…

Acquisizione di prove online

- Finalità: dimostrare che una risorsa online esiste in un certo periodo di tempo, mantenendo (per quanto possibile) i princìpi dell'Informatica Forense
  - Non alterabilità
  - Ripetibilità?
  - Hash?
- Ovviamente una stampa cartacea o PDF non basta
- Non è banale neanche "dimostrare" in modo oggettivo che qualcosa esista online, ma ci si può avvicinare all'oggettività

Princìpi della copia conforme da web

- Acquisire video di ciò che si fa
- Acquisire traffico di rete (Wireshark, tcpdump)
  - Se possibile, non cifrato (SSL, Proxy)
- Salvare codice integrale
- Contattare siti web esterni (ora esatta, newspaper, etc...)
- Eseguire traceroute, query dns, sync NTP, etc...
- Compattare il tutto, "congelare" con hash
- Apporre data certa (volendo anche tramite blockchain) ed eventualmente firmare

Problematiche dell'acquisizione siti web

- Alcuni parametri possono variare l'esito dell'acquisizione forense in particolare di siti web:
  - Indirizzo IP da cui proviene la richiesta
  - User Agent / tipo di browser
  - Sistema Operativo
  - Lingua
  - Orario
  - Aree protette o non indicizzate dai motori di ricerca

Acquisizione in-house di un sito web

- Attivare log e traccia query/response HTTP, dump di rete
- Whois, IP dell'hosting
- Certificati SSL, Dati DNS
- Acquisire tutto tramite crawler (es. wget)
  - Attenzione, anche robots.txt (controllare URL/path "disallow"), sitemap, eventuali RSS
- Se interessati, acquisire Google Serp (site: www.website.it) che può contenere pagine non linkate

Acquisizione in-house di un sito web

- Per una pagina:
  - wget --keep-session-cookies --save-cookies=cookies.txt --no-check-certificate -e robots=off -o log.txt -N -vv -S --no-remove-listing --preserve-permissions -np -E -k -K -p --user-agent="Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_5; en-us) AppleWebKit/525.26.2 (KHTML, like Gecko) Version/3.2 Safari/525.26.12" http://www.website.com/page.html
- Per un sito:
  - wget -m --keep-session-cookies --save-cookies=cookies.txt --limit-rate=500k -w 1 --random-wait --no-check-certificate -e robots=off -o log.txt -vv -S --preserve-permissions -np -E -k -K -p --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36" http://www.website.com/subdir

Problematiche

- Traffico cifrato con SSL (da ottobre, diventa un problema serio)
- Nazionalità di uscita
- User agent (OS ma anche browser: Mac OS, Windows, Linux ma anche Chrome, Firefox, Wget, Googlebot, etc…)
- Pagine dinamiche, html 5, AJAX (richiedono browser)
- Servizi che richiedono autenticazione
- Pagine rimosse dopo l'acquisizione o domini cancellati (utile DomainTools)

Acquisizione traffico di rete

- Con tcpdump:
  - (Mac OS) tcpdump -n -w out.pcap -i en0 -s 65535 host 192.168.0.9
  - (Linux con visualizzazione in tempo reale) tcpdump host xxx.xxx.xxx.xxx -s 65535 -w - | tee out.pcap | tcpdump -r –
- Con Wireshark
  - Impostare filtri su IP?
- Se si sta eseguendo operazione su PC di lavoro, si possono impostare filtri su processo
  - Mac: Little Snitch
- Se su macchina virtuale, fare dump di tutto

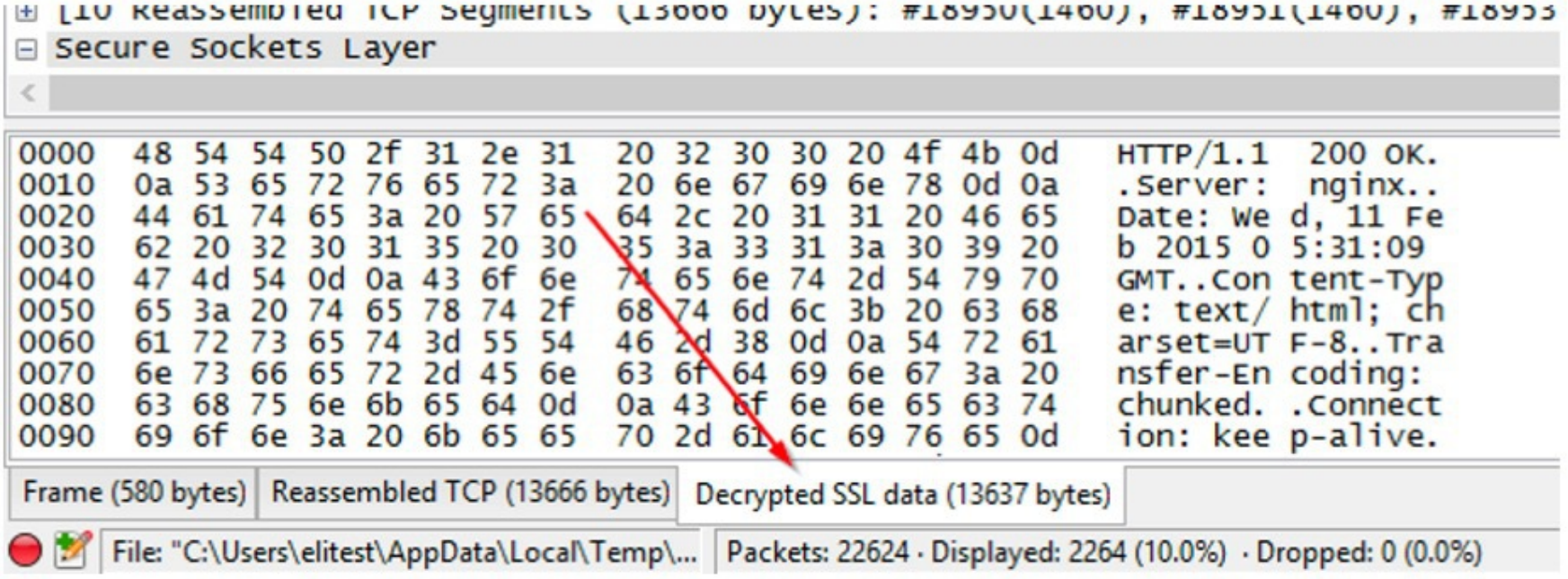
Acquisizione chiavi SSL

- Usare Firefox, su alcune versioni non funziona
- Windows:
  - computer properties "Advance system settings" "Environment Variables…"
  - Aggiungere variabile utente "SSLKEYLOGFILE" con percorso alla location del file txt
- Linux o Mac
  - export SSLKEYLOGFILE=/Users/username/sslkeylogs/output.log
  - open -a firefox
  - Wireshark
- Se interessano i certificati, usare le proprietà del browser oppure:
- Funziona anche con curl e con Thunderbird

Verifica acquisizione chiavi SSL

- https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/
- Avviare Wireshark, aprire le Preferenze, espandere sezione Protocols
- In (Pre) Master-Secret log filename inserire il path la file con le chiavi SSL
- Aprire il dump
- Nei pacchetti con SSL, visualizzare tab in basso "Decrypted SSL data"

Verifica acquisizione chiavi SSL



La soluzione in-house

- Creare macchina virtuale con Ubuntu Mint
- Configuro Wireshark/Tcpcdump e un browser che lancio con SSLKEYLOGFILE
- Avvio registrazione (host o guest)
- Avvio dump di rete
- Finita la visita e il salvataggio, compatto macchina virtuale in ZIP, calcolo hash, appongo data certa, verbalizzo,consegno

Soluzioni commerciali

- Alcuni Servizi
  - Legaleye (legaleye.cloud)
  - Giuffré Cliens
  - Chi Odia Paga
  - Safe Stamper (www.safestamper.com)
  - PageFreezer (pagefreezer.com)
- Alcuni Tool
  - X1 Social Discovery
  - FAW
  - Oxygen Forensics

Attività integrative ed esempi pratici

- Acquisire anche con servizi terzi, gratuiti:
  - Web.archive.org (**attenzione**, rimane online, non indicizzato)
  - Archive.is (**attenzione attenzione**, rimane online, **indicizzato**, rimuovono su richiesta ma sono lenti), si può scaricare dump
  - Perma.cc (rimane online, anche in modo privato), si scarica dump
  - webrecorder.io (remote browser, si scarica dump)
    - github.com/webrecorder/webrecorderplayer-electron
  - freezepage.com
- Certificare con **hashbot**
  - Scegliere user agent
  - Scaricare dump

Acquisizione email

- In ogni caso, acquisire mail integrale in formato RFC822
- Diversi tipi di acquisizione:
  - Webmail (con download source)
  - POP3
  - IMAP4
- Se acquisizione webmail, necessario loggarsi:
  - VM
  - FAW
  - Servizi commerciali con browser remoto

Acquisizione email

- Prodotti commerciali:
  - Forensic Email Collector
  - Securcube Downloader
  - Aid4Mail
  - Oxygen Forensiscs (Cloud)
  - Axiom Cloud

Contatti

paolo@dalchecco

www.dalchecco.it

@forensico