DIGITALNA FORENZIKA

prof. dr Saša Adamović
sadamovic@singidunum.ac.rs

Forenzička istraga operativnih sistema

UNIVERZITET PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Operativni sistem

- Pruža softversku platformu za pokretanje drugih programa.
- OS je odgovoran za:
  - obradu ulaznih komandi UI,
  - slanje izlaza na ekran,
  - učestvuje u interakciji sa uređajima za skladištenje i preuzimanje podataka,
  - kontrolu perifernih uređaja (štampači i modemi)
- Postoje različiti OS:
  - Windows, Linux, UNIX i MAc OS.

PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Periferije - operativni sistem

- Mrežni uređaji, mobilni uređaji, digitalne kamere, audio plejeri i mobilni telefoni, takođe koriste OS.
- Postoje dve vrste podataka na OS:
  - podaci koji postoje nakon gašenja računara (održivi),
  - podaci koji ne postoje nakon gašenja računara (neodrživi).
- Upravo ove dve kategorije su od velikog interesa za vođenje forenzičkog postupka.

PRVI AKREDITOVANI PRIVATNI UNIVERZITET UNIVERZITET SINGIDUNUM

Održivi podaci

- Primarni izvor ovakvih podataka na OS je filesystem.
- *Filesystem* je jedan od informaciono najbogatijih izvora za digitalnog forenzičara.
- Sledi nekoliko vrsta podataka koje je moguće pronaći u OS *filesystem-u*:
- ***Configuration files*** poseduju informacije o listi servisa za startovanje, lokaciji log i privremenih fajlova, kao i o hardverskim podešavanjima (štampači, rezolucija, itd..)
  - **Korisnici i grupe**
    - član grupe
    - naziv korisničkog naloga
    - privilegije
    - status naloga
  - **Fajl sa lozinkama**
    - heš vrednosti lozinki
  - **Planeri**
    - softverska ažuriranja

UNIVERZITET PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Održivi podaci

- ***Logs files*** sadrže informacije o raznim događajima na OS i događajima vezanim za aplikacije.
- Tipovi informacija:
  - ***System events*** - svi događaji vezani za OS
  - ***Audit records*** - uspešna/neuspešna provera identiteta
  - ***Application events*** - promene konfiguracije OS
  - ***Command history*** - istorija komandi za svakog korisnika
  - ***Recently accessed files*** - hronološka lista fajlova kojima se pristupalo

PRVI AKREDITOVANI UNIVERZITET SINGIDUNUM

Održivi podaci

- ***Application files*** – sadrže različite tipove podataka:
  - Izvršne skripte
  - Dokumentaciju
  - Konfiguracione fajlove
  - Log fajlove
  - Istoriju datoteke
  - Slike
  - Zvukove
  - Dokumentaciju

UNIVERZITET PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Održivi podaci

- ***Data files*** **–** Sadrže skladištene informacije za aplikaciju.
- Uobičajne datoteke:
  - Tekstualni fajlovi
  - Tabele
  - Baze podataka
  - Audio fajlove
  - Grafičke fajlove
- Primer: kada se štampa neki dokument, većina OS kreira jedan ili više privremenih fajlova sa pripremom za štampu.

UNIVERZITET PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Održivi podaci

- ***Swap files*** **–** Uloga svap fajlova je da proširi RAM memoriju. Koristi se za privremeno skladištenje podataka.
- Svap fajlovi sadrže:
  - Informacije o OS
  - Informacije o aplikaciji
  - Korisnička imena
  - Heševe lozinki
  - Kontakt informacije

UNIVERZITET PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Održivi podaci

- ***Dump files*** **–** Fajlovi podataka koji nastaju u momentu nastanka greške u radu neke aplikacije (radi rešavanja problema).
- ***Hibernation files***– čuvaju informaciju o trenutnom stanju sistema. Beleži stanje memorije i otvorenih fajlova.
- ***Temporary files***– Tokom instalacije softvera na OS se kreiraju privremeni fajlovi koji se nakon uspešnog procesa automatski brišu. Ovi fajlovi ne budu obrisani uvek, a mogu da sadrže različite tipove informacija.

AKREDITOVANI UNIVERZITET SINGIDUNUM

Neodrživi podaci

- Podaci u RAM memoriji.
- Podaci se konstantno menjaju u toku rada OS.
- ***RAM Slack space*** **–** Slično kao i kod drugih medija, aplikacije nekad zahtevaju više memorije nego što stvarno koriste (bolje performanse).
- ***RAM Free space*** – Slično kao i kod drugih medija, memorijski prostor je oslobođen, ali i dalje se nalaze podaci u vidu smeća.

PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Neodrživi podaci

- Postoje i drugi izvori neodrživih podataka na OS.
- ***Network configuration*** – IP adrese, domen.
- ***Network connections*** – analiza ip adrese i portova za dolazni i odlazni saobraćaj na OS-u
- ***Running processes*** – na osnovu liste OS procesa moguće je analizirati ponašanje korisnika.
- ***Open files*** – analiza OS liste otvorenih fajlova.
- ***Login sessions*** – informacije o trenutno logovanim korisnicima, trajanju sesije, praćenje navika korisnika, analiza aktivnosti korisnika u vreme događaja.
- ***Operating system time*** - tačno vreme i vremenske zone, vreme na OS i vreme u BIOS-u mogu da se razlikuju zbog vremenskih zona.

UNIVERZITET SINGIDUNUM PRVI AKREDITOVANI PRIVATNI UNIVERZITET

Prikupljanje podataka sa OS slučaj: neodrživi podaci

- Prikupljanje podataka sa najmanjim izmenama sistema.
- Upotreba forenzičkih alata sa CD-a ili USB fleša neće izazvati promenu na sistemu.
- Forenzički alati ne garantuju tačnost podataka.
- Analitičar treba da poznaje rad svakog alata i u kojoj meri ostvaruje interakciju sa OS.
- Neki važni tipovi neodrživih podataka:
  - Contents of memory (kopiranje RAM memorije)
  - Network configuration (kopiranje ipconfig ili ifconfig)
  - Network connections (kopiranje netstat konfiguracije)

PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Prikupljanje podataka sa OS
Slučaj: neodrživi podaci

- Preporučeni forenzički alati:
  - *OS Command Prompt* (obezbeđuje komandni prozor za izvršenje drugih alata)
  - *SHA-1 Checksum* (obezbeđenje servisa za verifikaciju integriteta podataka preko SHA-1 heš funkcije)
  - *Directory List* (generisanje listinga svih direktorijuma u fajl sistemu, primer: Windows DIR ili UNIX LS)
  - *String Search* (identifikovanje fajlova od interesa na osnovu pretrage zadatog stringa)
  - *Text Editor* (alat koji može da bude zgodan za pregled sadržaja nekog fajla)

PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Prioriteti u procesu prikupljanja neodrživih podataka na OS-u

- Prioritet prikupljanja neodrživih podataka zavisi od konkretnog događaja (upad u mrežu – mrežna konfiguracija, mrežne konekcije i sesije).
- Neodrživi podaci mogu da se menjaju vremenom.
- Preporučuje se sledeći redosled prikupljanja podataka:
  1. *Network connections*
  2. *Login sessions*
  3. *Contents of memory*
  4. *Running processes*
  5. *Open files*
  6. *Network configuration*
  7. *Operating system time.*

UNIVERZITET PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Prikupljanje podataka sa OS
Slučaj: održivi podaci

- Proces sledi nakon prikupljanja neodrživih podataka.
- Analitičar procenjuje momenat kada će isključiti računar.
- Isključenje se može obaviti na dva načina:
- Standardna opcija Shutdown
  - zatvaranje otvorenih fajlova
  - brisanje privremenih fajlova
  - eventualno čišćenje swap fajlova
  - uklanjanje zlonamernog softvera
- Uklanjanje kabla za napajanje
  - čuvanje podataka u swap fajlu
  - čuvanje privremenih fajlovi sa podacima koji bi mogli biti izgubljeni tradicionalnim gašenjem računara
  - moguć gubitak podataka (otvoreni fajlovi)

UNIVERZITET PRVI AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

Prikupljanje podataka sa OS
Slučaj: održivi podaci

- Koraci posle isključenja računra:
  - popisati sve hardverske komponente
  - popisati sve kablove i interfejse sa drugim periferijama
  - sve dokumentovati i fotografisati
  - koristiti antistatičke rukavice
- Lista održivih izvora podataka za analizu:
  - *Users and groups* (analiza korisnika)
  - *Passwords* (prikupljanje heševa)
  - *Network shares* (analiza deljenih lokalnih resursa)
  - *Logs* (informacije o uspešnosti logovanja na OS)

UNIVERZITET SINGIDUNUM PRVI AKREDITOVANI PRIVATNI UNIVERZITET

Zaključak

1. Analitičar treba da izabere adekvatne metode radi očuvanja neodrživih podataka.
2. Odluke moraju biti brzo donešene.
3. Potrebno je proceniti moguće rizike u pogledu važnosti potencijalno pribavljene informacije.
4. Analitičar treba da koristi forenzički alat za prikupljanje neodrživih podataka na OS-u.
5. Upotreba odgovarajućih alata umanjuje mogućnost za ometanje OS-a.
6. Analitičar treba da zna kako izabrani forenzički alat utiče na promene OS-a.
7. Analitičar treba da izabere odgovarajući metod za gašenje računara.
8. Savki metod gašenja može da izazove različito ponašanje OS-a, što može da izazove oštećenje ili gubljenje podataka.

AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM