



# Introducere în Analiza Capturilor de Date, Trafic de Rețea, Memorie sau Hard Disk (forensics)

Resurse utile pentru incepatori din UNbreakable România

[unbreakable.ro](http://unbreakable.ro)

<b>Declinarea responsabilității</b>	<b>3</b>
<b>Introducere</b>	<b>4</b>
Ce poate fi investigat într-un incident informatic?	4
Ce este criminalistica digitală?	4
Obiectivele criminalisticii computerizate	5
Pașii procesului de criminalistică digitală	5
Tipuri de criminalistică digitală	6
1. Disk forensics	6
2. Networking forensics	6
3. Wireless forensics	7
3.1 Pașii de execuție a unui proces de forensics pentru sisteme wireless	7
4. Criminalistica digitală a bazelor de date	8
5. Criminalistica digitală pentru malware	8
5.1 Tipuri de malware	8
5.2 Simptome prezentate de un sistem infectat	8
5.3 Diferite moduri în care programele malware pot intra în sistem:	9
6. Criminalistica digitală pentru servicii de tip e-mail	9
7. Criminalistică digitală pentru memorie	9
7.1 Ce este un dump de memorie?	10
7.2 Ce este memoria volatilă?	10
8. Criminalistică digitală pentru dispozitivelor mobile	10
9. Criminalistică digitală pentru rețele de calculatoare	10
Provocări cu care se confruntă criminalistica digitală	11
Exemple de utilizare a criminalisticii digitale	11
Avantajele criminalisticii digitale	11
<b>Librarii si unelte utile în rezolvarea exercițiilor</b>	<b>12</b>
<b>Exerciții și rezolvări</b>	<b>13</b>
Zanger (usor)	13
HiddenTypo (mediu)	14
Not-clear (mediu - ridicat)	17
<b>Contribuitori</b>	<b>21</b>

## Declinarea responsabilității

Aceste materiale și resurse sunt destinate exclusiv informării și discuțiilor, având ca obiectiv conștientizarea riscurilor și amenințarilor informatice dar și pregătirea unor noi generații de specialiști în securitate informatică.

Organizatorii și partenerii UNbreakable România nu oferă nicio garanție de niciun fel cu privire la aceste informații. În niciun caz, organizatorii și partenerii UNbreakable România, sau contractanții, sau subcontractanții săi nu vor fi răspunzători pentru niciun fel de daune, inclusiv, dar fără a se limita la, daune directe, indirecte, speciale sau ulterioare, care rezultă din orice mod ce are legătură cu aceste informații, indiferent dacă se bazează sau nu pe garanție, contract, delict sau altfel, indiferent dacă este sau nu din neglijență și dacă vătămarea a fost sau nu rezultată din rezultatele sau dependența de informații.

Organizatorii UNbreakable România nu aprobă niciun produs sau serviciu comercial, inclusiv subiectele analizei. Orice referire la produse comerciale, procese sau servicii specifice prin marca de servicii, marca comercială, producător sau altfel, nu constituie sau implică aprobarea, recomandarea sau favorizarea acestora de către UNbreakable România.

Organizatorii UNbreakable România recomandă folosirea cunoștințelor și tehnologiilor prezentate în aceste resurse doar în scop educațional sau profesional pe calculatoare, site-uri, servere, servicii sau alte sisteme informatice doar după obținerea acordului explicit în prealabil din partea proprietarilor.

Utilizarea unor tehnici sau unelte prezentate în aceste materiale împotriva unor sisteme informatice, fără acordul proprietarilor, poate fi considerată infracțiune în diverse țări.

În România, accesul ilegal la un sistem informatic este considerată infracțiune contra siguranței și integrității sistemelor și datelor informatice și poate fi pedepsită conform legii.

# Introducere

**Criminalistica digitală (forensics) și securitatea cibernetică merg mână în mână; securitatea cibernetică nu ar fi la fel de importanta dacă nu ar fi informațiile furnizate de criminalistica digitală.**

Pentru a da o definiție formală, criminalistica digitală (denumită și criminalistică informatică sau cyber-criminalistică) este practica colectării, analizei și raportării informațiilor găsite pe computere și rețele, în așa fel încât acest proces să fie considerat admisibil într-un context juridic - fie ca dovadă într-o anchetă penală sau civilă, fie ca dovadă documentară într-un cadru comercial sau privat.

Securitatea cibernetică preia informațiile pe care criminalistica digitală le-a găsit în diferite cazuri și creează modalități de prevenire a incidentelor de securitate.

Securitatea cibernetică este în esență proactivă în vreme ce criminalistica digitală este reactivă.

## Ce poate fi investigat într-un incident informatic?

**Orice aplicatie sau activitate realizata pe un sistem informatic lasa urme**, mai ales cand sunt realizate imbunatatiri ale capacitatii de detectie sau jurnalizare a activitatilor suspecte sau malitioase.

Intr-un incident informatic este foarte important sa colectezi si sa documentezi cat mai detaliat dovezile care vor ajuta la alcatuirea unei naratiuni pentru eveniment, ce va include elemente cu privire la modul in care s-a declansat incidentul, care au fost consecintele, daca amenintarea inca exista samd.

Aceste dovezi pot fi obtinute in mai multe moduri:

- Prin analiza unei capturi de memorie volatila (de eg. RAM)
- Prin analiza unei capturi de trafic de retea
- Prin analiza unei capturi a sistemelor de stocare (eg. HDD, USB samd)
- Prin analiza unor jurnale (logs) generate de sistemele de operare, aplicatii samd

## Ce este criminalistica digitală?

Criminalistica digitală este definită ca procesul de conservare, identificare, extragere și documentare a dovezilor computerizate care pot fi utilizate de instanța de judecată.

Criminalistica digitală este știința găsirii dovezilor din media digitală, cum ar fi un computer, telefon mobil, server sau rețea.

## Obiectivele criminalisticii computerizate

Printre obiectivele esențiale ale utilizării criminalisticii computerizate, putem enumera:

- Ajută la recuperarea, analiza și conservarea computerelor și a materialelor conexe în așa fel încât ajută echipa anchetatoare să le prezinte ca probe în instanță de judecată.
- Proiectarea procedurilor la locul suspectat al incidentului care vă ajută să vă asigurați că dovezile digitale obținute nu sunt corupte.
- Achiziționarea și duplicarea datelor:
  - recuperarea fișierelor șterse și partițiilor șterse de pe suportul digital pentru a extrage dovezile și a le valida.
- Vă ajută să identificați rapid dovezile și, de asemenea, vă permite să estimați impactul potențial al activității dăunătoare asupra victimei
- Realizarea unui raport criminalistic computerizat care oferă o perspectivă completă asupra procesului de investigație.
- Conservarea probelor urmărind lanțul de custodie.

## Pașii procesului de criminalistică digitală

Procesul de criminalistică digitală presupune următorii pași:

- **Identificare**
  - Este primul pas în procesul criminalistic.
  - Procesul de identificare include în principal lucruri precum:
    - ce dovezi sunt prezente
    - unde sunt stocate
    - cum sunt stocate (în ce format).
  - Mediile de stocare electronice pot fi calculatoare personale, telefoane mobile, PDA-uri etc.
- **Conservare**
  - În această fază, datele sunt izolate, securizate și conservate.
  - Acest pas de asemeni presupune și împiedicarea utilizării dispozitivului digital, astfel încât dovezile digitale să nu fie modificate.
- **Analiză**
  - În această etapă, agenții de investigație reconstituie fragmente de date și trag concluzii pe baza dovezilor găsite.
- **Documentație**
  - În acest moment, se realizează o înregistrare a tuturor datelor vizibile pentru o revizuire cât mai exactă asupra evenimentelor din timpul crimei.
- **Prezentare**
  - În acest ultim pas, se construiesc concluziile bazate pe informațiile adunate în etapele anterioare.

## Tipuri de criminalistică digitală

Putem enumera mai multe tipuri principale de criminalistică digitală:

### 1. Disk forensics

Se ocupă cu extragerea datelor din mediile de stocare prin căutarea fișierelor active, modificate sau șterse.

Dispozitivele digitale sunt baza multor operații din viața noastră, prin urmare, dovezile digitale, sunt din ce în ce mai utilizate în investigații.

O caracteristică importantă a dovezilor digitale este că pot fi ușor deteriorate sau distruse. Adesea, acest lucru se întâmplă neintenționat. De exemplu, atunci când personalul tehnic încearcă să restabilească o rețea de calculatoare, după un incident, iar o sursă validă de dovezi digitale este în acest caz, un hard disk.

### Tipuri de copii legale

Există două tipuri principale de copii legale:

- Copiere de tip „drive to drive” - atunci când datele achiziționate de pe un hard disk (sursa digitală) sunt transferate pe altul.
- Copiere de tip „drive în fișier” - atunci când datele achiziționate de pe un hard disk (sursa digitală) sunt transferate într-un fișier situat pe o altă unitate.
  - Acest lucru creează o copie sector-pe-sector a hard disk-ului în studiu.
  - De obicei, această imagine are formatul DD (RAW) sau Encase (E01). Formatul DD este un fișier care conține o copie a datelor de pe disc.

### 2. Networking forensics

Este o subcategorie a criminalisticii digitale și reprezintă monitorizarea și analiza traficului din rețeaua de calculatoare pentru a colecta informații importante și dovezi legale.

Acest proces se referă la investigarea și analiza întregului trafic care traversează o rețea suspectată a fi folosită cu scop malițios, în răspândirea malware-ului care fură date sau susține alte atacuri cibernetice.

Analistii vor căuta date care indică comunicarea umană, manipularea fișierelor și utilizarea anumitor cuvinte cheie, etc.

Cu ajutorul acestei metodologii, anchetatorii legii și criminalistica cibernetică pot urmări comunicațiile și stabili cronologii pe baza evenimentelor de rețea înregistrate de sistemele de control.

În afara investigațiilor penale, organizațiile aplică diferite metode de analiză a traficului de date între anumite rețele pentru a depista anomalii, artefacte, tentative de atac în sistemele de operare.

Spre deosebire de criminalistica digitală computerizată, analiza traficului este mai dificil de realizat, deoarece datele sunt adesea transmise prin rețea și apoi pierdute; în criminalistica computerelor, datele sunt păstrate de multe ori pe disc sau pe hardware extern, ceea ce le face mai ușor de obținut.

Este demn de remarcat faptul că legile privind confidențialitatea și protecția datelor restricționează o anumită urmărire și analiză activă a traficului de rețea, fără permisiunea explicită, deci dacă intenționați să aplicați instrumentele de criminalistică în rețea, fiți conștienți că trebuie să respectați legile privind confidențialitatea datelor.

Criminalistica digitală asupra rețelelor poate fi, de asemenea, utilizată într-un mod proactiv pentru a descoperi defectele din infrastructura IT, oferind astfel administratorilor și ofițerilor de securitate a informațiilor, posibilitatea de a-și consolida apărarea împotriva viitoarelor atacuri cibernetice.

### 3. Wireless forensics

Este o subdivizie a categoriei network forensics, iar scopul principal al acestui proces este de a oferi instrumentele necesare pentru colectarea și analiza datelor din traficul dintr-o rețea wireless.

Criminalistica digitală pentru sistemele wireless, a fost recunoscută în prezent ca o provocare majoră atât pentru organizațiile tehnice, cât și pentru cele juridice; creșterea rețelelor wireless și a dispozitivelor de acces au creat mai multe vulnerabilități de securitate și au dus la mai multe incidente și amenințări atât pentru organizații, cât și pentru consumatori. În timp ce există metodologii, tehnici și instrumente de actualitate care sunt utilizate sau în curs de dezvoltare în acest domeniu, provocarea rămâne față de evoluția rapidă a tehnologiilor de acest tip.

#### 3.1 Pașii de execuție a unui proces de forensics pentru sisteme wireless

Pentru a efectua un proces de forensics adecvat unui sistem wireless, trebuie mai întâi să colectăm și să analizăm traficul Wi-Fi. Apoi, următorul pas este să evaluăm performanța rețelei pentru a detecta anomaliiile și utilizarea necorespunzătoare a resurselor, protocoalele de rețea folosite, agregarea datelor din mai multe surse și răspunsurile la incidente.

Procesul, conform triumghiului criminalistic CIA, constă din trei părți.

#### 1. Captura

În acest moment se realizează captura traficului de internet, pentru a fi ulterior studiat, aplicând diferite metodologii de lucru.

## 2. Identificare

În acest moment, pachetele sunt identificate și filtrate corespunzător în funcție de oră și dată.

## 3. Analiză

Pachetele sunt reconstituite și clasificate în funcție de tipul și antetul lor.

## 4. Criminalistica digitală a bazelor de date

Este o ramură a criminalisticii digitale referitoare la studiul și examinarea bazelor de date și a metadatelor aferente acestora.

Această metodologie este similară cu criminalistica computerizată, iar o examinare a unei baze de date se poate construi pe baza marcajelor de timp ce determină succesiunea acțiunilor unui utilizator, într-o perioadă definită. Alternativ, o examinare criminalistică se poate concentra pe identificarea tranzacțiilor dintr-un sistem de baze de date sau o aplicație care indică dovezi ale acțiunilor efectuate, cum ar fi un caz de fraudă.

## 5. Criminalistica digitală pentru malware

Această ramură se ocupă cu identificarea codului malițios, pentru înțelege cât mai bine structura programelor infectate cu diferiți viruși.

Prin această metodă de analiză și investigare, se pot identifica diferite proprietăți ale malware-ului pentru a găsi vinovații și motivul atacului.

Procesul include, de asemenea, sarcini precum identificarea codului malițios, metoda de propagare a acestuia, impactul asupra sistemului, porturile pe care încearcă să le utilizeze etc.

### 5.1 Tipuri de malware

- Backdoor
- Botnet
- Downloader
- Launcher
- Rootkit
- HackTool
- Rogue application
- Scareware
- Worm sau Virus
- Credential-stealing program, etc

### 5.2 Simptome prezentate de un sistem infectat

Printre efectele vizibile ce apar în urma unei infestări de tip malware, putem enumera:



- Este posibil ca sistemul să devină instabil și să răspundă încet, deoarece programele malware folosesc resursele necesare unei execuții rapide.
- Executabile necunoscute instalate pe sistem.
- Trafic de rețea neașteptat către site-uri străine.
- Setări de sistem modificate, cum ar fi pagina de pornire a browserului, fără acordul dvs.
- Ferestrele pop-up aleatorii ce sunt afișate ca reclame.
- Sunt afișate mesaje precum „Computerul dvs. este infectat” și solicită utilizatorului să furnizeze o anumită sumă de bani, sau să fie îndeplinite alte condiții pentru recuperarea datelor personale.
- În general, sistemul va prezenta un comportament neașteptat și imprevizibil.

### ***5.3 Diferite moduri în care programele malware pot intra în sistem:***

- Aplicații de mesagerie instant
- Dispozitive detașabile
- Linkuri și atașamente ce sunt accesate din interiorul e-mailurilor primite
- Bug-uri pentru browser și e-mail
- NetBIOS
- Programe false
- Site-uri de torrente și software freeware
- Descărcarea fișierelor, a jocurilor și a diferitelor aplicații din surse necunoscute.

## **6. Criminalistica digitală pentru servicii de tip e-mail**

Se ocupă cu recuperarea și analiza e-mailurilor, inclusiv a e-mailurilor șterse, a calendarelor și a contactelor.

## **7. Criminalistică digitală pentru memorie**

Se ocupă cu colectarea datelor din memoria sistemului (registre de sistem, cache, RAM) sub formă brută și apoi analizarea datelor din dump-ul Raw.

Un proces de forensics pentru memorie poate oferi informații unice despre activitatea sistemului de execuție, inclusiv conexiuni de rețea deschise și comenzi sau procese executate recent.

În multe cazuri, datele critice ce fac referință la amenințările sau atacurile cibernetice efectuate, vor exista exclusiv în memoria sistemului.

Aici putem include exemple precum: conexiuni de rețea, acreditări de cont, mesaje de chat, chei de criptare, procese care rulează, fragmente de cod injectate și istoricul internetului care nu poate fi ascuns în cache. Orice program malițios sau de altă natură - trebuie încărcat în memorie pentru a putea fi executat, iar acest aspect constituie importanța majoră a unui proces de forensics, deoarece este metoda prin care anchetatorii pot obține informațiile necesare în a înțelege un atac și măsurile de protecție ce trebuiesc ulterior implementate.

### 7.1 Ce este un dump de memorie?

Un dump de memorie (cunoscut și sub numele de dump de bază sau dump de sistem) este o captură instantanee a datelor de memorie ale computerului dintr-un moment specific. Acest dump de memorie poate conține date valoroase pentru un proces de criminalistică digitală, spre exemplu date despre starea sistemului înainte de un incident.

### 7.2 Ce este memoria volatilă?

Datele volatile sunt datele stocate în memoria temporară, pe un computer în timp ce rulează. Când un computer este oprit, datele volatile se pierd aproape imediat.

Datele volatile se află în memoria de stocare pe termen scurt a unui calculator și pot include date precum istoricul de navigare, mesaje de chat și conținut din clipboard. Dacă, de exemplu, ați lucra la un document în Word, ce nu a fost salvat încă pe hard disk sau într-o altă sursă de memorie nevolatilă, atunci v-ați pierde munca dacă computerul ar pierde ar suferi o pană de curent.

## 8. Criminalistică digitală pentru dispozitivelor mobile

Se ocupă în principal cu examinarea și analiza dispozitivelor mobile. Ajută la recuperarea contactelor telefonice și SIM, jurnale de apeluri, SMS / MMS, audio, video etc.

Telefoanele mobile ocupă un loc important în criminalistica digitală, datorită utilizării lor pe scară largă, atât de persoane fizice, dar și de corporații. Importanța examinării datelor numite drept dovezi în cazul telefoanelor mobile a crescut odată cu progresele în tehnologie și capacitatea de funcționare, stocare, funcționalitate. Într-un caz de criminalistică, telefoanele mobile trebuie examinate de către persoane autorizate, iar datele obținute de pe dispozitiv trebuie procesate în conformitate cu anumite standarde din acest domeniu de activitate.

## 9. Criminalistică digitală pentru rețele de calculatoare

Tratează o gamă largă de informații digitale din jurnalele de sistem, cum ar fi istoricul browserului, loguri de sistem și alte file ce sunt stocate pe mașina în analiză.

Anchetatorii urmează de obicei un set standard de proceduri: după izolarea fizică a dispozitivului în cauză, ce elimină riscul contaminării accidentale, anchetatorii fac o copie digitală a mediului de stocare al dispozitivului. Odată ce suportul original a fost copiat, acesta este blocat într-un loc sigur pentru a-și menține starea intactă.

Toate investigațiile se fac pe copia digitală, iar analiza presupune o varietate de tehnici și aplicații software pentru a examina copia, căutând în folderele ascunse și în spațiul de pe disc nealocat, copii ale fișierelor șterse, criptate sau deteriorate. Orice dovadă găsită pe copia digitală este documentată cu atenție într-un „raport de constatare” și este verificată împreună cu originalul.

Criminalistica digitală computerizată s-a dezvoltat foarte mult în ultimii ani, odată cu evoluția tehnologiilor din diverse domenii ce funcționează pe baza rețelelor de calculatoare.

## **Provocări cu care se confruntă criminalistica digitală**

În ziua de azi, criminalistica digitală se confruntă cu următoarele provocări:

- Creșterea numărului de PC-urilor deținute de persoane fizice, companii și extinderea accesului la internet
- Disponibilitate ușoară asupra instrumentelor de hacking ce pot fi descărcate gratuit din diferite surse publice.
- Lipsa dovezilor fizice îngreunează urmărirea penală.
- Cantitatea mare de spațiu de stocare în Terabytes care îngreunează această activitate de investigație.
- Orice schimbări tehnologice necesită o reactualizare a metodelor de operare a unui proces de criminalistică digitală.

## **Exemple de utilizare a criminalisticii digitale**

În ultima perioadă, organizațiile comerciale au folosit criminalistica digitală în identificarea și analiza următoarelor cazuri:

- Furt de proprietate intelectuală
- Spionaj industrial
- Conflicte din spațiul locului de muncă
- Anchete de fraudă
- Utilizarea necorespunzătoare a internetului și a emailului la locul de muncă
- Probleme legate de falsuri
- Investigații falimentare

## **Avantajele criminalisticii digitale**

Printre avantajele criminalisticii digitale, putem enumera:

- asigura integritatea sistemului computerizat.
- Poate obține probe valide, ce aduse în instanță, pot duce la pedepsirea vinovatului.
- Ajută companiile să capteze informații importante despre sistemele sau rețelele lor de calculatoare, atunci când acestea sunt compromise.
- Urmărește în mod eficient criminalii cibernetici de oriunde din lume.
- Ajută la protejarea datelor și bunurilor unei organizații.
- Permite extragerea, procesarea și interpretarea probelor de fapt, astfel încât să demonstreze acțiunea atacului cibernetic în instanță.

## Librarii si unelte utile în rezolvarea exercițiilor

- [Wireshark](#) - analiza pachetelor de date
- [Volatility Framework](#) - analiza capturilor de memorie (eg. RAM)
- dd - utilitar pentru crearea unor imagini de disc prin copierea low-level a datelor
- [Aircrack-ng](#) - utilitar pentru exploatarea vulnerabilitatilor Wireless
- [Audacity](#) - utilitar recomandat pentru analize audio
- [Exif tools](#) - utilitar pentru a vizualiza sau edita headerele imaginilor

# Exerciții și rezolvări

## Zanger (usor)

Concurs: UNbreakable #1 (2020)

Descriere:

```
One communications protocol over certain ports to rule them all.  
  
Flag format: ctf{sha256}  
  
Goal: In this challenge you receive a capture dump and your goal is to find the  
attacker techniques used to leak the flag.  
  
The challenge was created by Bit Sentinel.
```

Rezolvare:

După deschiderea fișierului **pcap** oferit pe pagina exercițiului în **WireShark**, putem observa doua tipuri de pachete: UDP si TCP. Cum în fișier sunt prezente 138 de pachete de tip TCP ( $\text{len(flag)} * 2$ ), le extragem cu **tsark** într-un fișier pentru a le interpreta:

```
yakuhito@furry-catstation:~/ctf/unbr1/zanger$ tshark -r flag.pcap -Y "tcp"  
-e tcp.dstport -Tfields > a  
yakuhito@furry-catstation:~/ctf/unbr1/zanger$ python solve.py  
ctf{2f0e53fae2572c358b82bdddf6d02b4a5315cc453d2d9a1df7914bdf6e61aa{  
yakuhito@furry-catstation:~/ctf/unbr1/zanger$
```

Cum știm că primele caractere ale flag-ului sunt **ctf{**, putem deduce ușor regula după care caracterele sunt transformate in numere din primele 4 porturi prezente în fișier:

```
arr = open("a", "r").read().split("\n")[:-1]  
arr = [int(i) for i in arr]  
  
flag = ""  
i = 0  
while i < len(arr):  
    if arr[i + 1] == 1337:
```

```
        flag += chr(arr[i] * 16 + 0xb)
    else:
        flag += chr(arr[i] * 16 + arr[i + 1])
    i += 2

print(flag)
```

Rezolvare în engleză: <https://blog.kuhi.to/unbreakable-romania-1-writeup#zanger>

## HiddenTypo (mediu)

Concurs: UNbreakable #2 (2020)

Descriere:

A group of unethical hackers managed to extract the secret ticket needed to unlock the safe, from the director's computer.

All we have is this file dump .. can you please help ?

Flag format: ctf{sha256}

Rezolvare:

Fișierul atașat exercițiului este un **memory dump** pe care îl putem citi folosind programul **volatility**. Primul pas este sa determinam tipul de sistem pe care a fost făcut dump-ul:

```
yakuhito@furry-catstation:~/ctf/unr2/hiddentypo$ volatility imageinfo -f
admin.bin
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64,
Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
           AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
           AS Layer2 : FileAddressSpace
(/home/yakuhito/ctf/unr2/hiddentypo/admin.bin)
PAE type  : No PAE
```

```
DTB : 0x187000L
KDBG : 0xf800028020a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xffffffff80002803d00L
KUSER_SHARED_DATA : 0xffffffff7800000000L
Image date and time : 2020-12-08 12:26:00 UTC+0000
Image local date and time : 2020-12-08 04:26:00 -0800
yakuhito@furry-catstation:~/ctf/unr2/hiddentypo$
```

După cum se poate vedea în output-ul comenzii de mai sus, profilul imaginii este **Win7SP1x64**. Acum ca avem profilul, putem începe să analizăm dump-ul prin listarea fișierelor existente pe hard disk:

```
yakuhito@furry-catstation:~/ctf/unr2/hiddentypo$ volatility -f admin.bin
--profile=Win7SP1x64 filescan > files
Volatility Foundation Volatility Framework 2.6
yakuhito@furry-catstation:~/ctf/unr2/hiddentypo$ cat files | grep .png
0x000000007de21530      16      0 R--r-- \Device\HarddiskVolume2\Program
Files\Windows Media Player\Network Sharing\wmpnss_color48.png
0x000000007e045970      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (3).png
0x000000007e04c970      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (2).png
0x000000007e1eedd0      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (11).png
0x000000007e3e1dd0      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (5).png
0x000000007e3e3d10      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy.png
0x000000007fc86e60      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (17).png
0x000000007fc8f070      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (18).png
0x000000007fc987d0      16      0 R--r-d
\Device\HarddiskVolume2\Users\target\Desktop\ticket.png
0x000000007fc9a640      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (7).png
0x000000007fcb2960      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (16).png
```

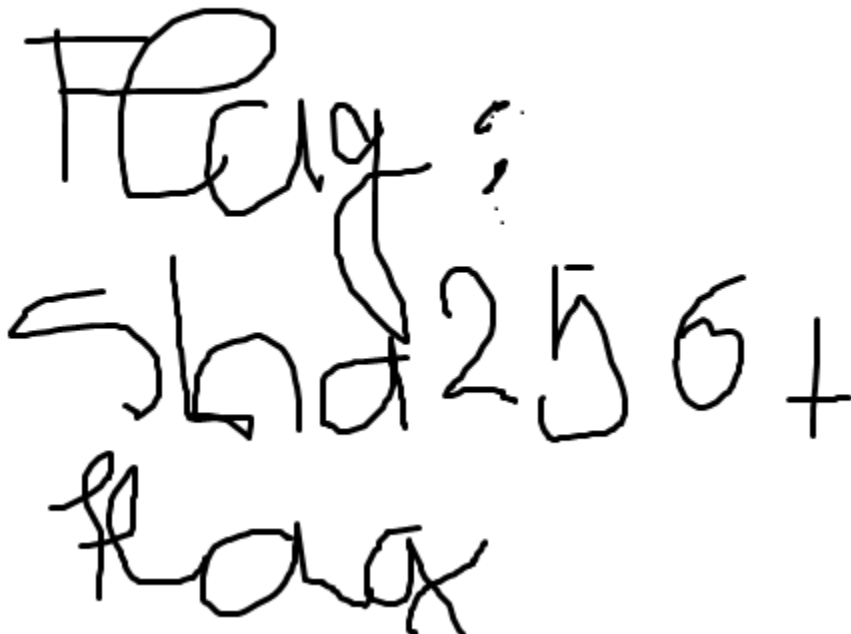
```
0x000000007fcb2d60      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (12).png
0x000000007fcb9890      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (14).png
0x000000007fcbe070      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (8).png
0x000000007fcbed90      16      0 RW----
\Device\HarddiskVolume2\Users\target\Documents\ticket.png
0x000000007fcc4a80      16      0 RW----
\Device\HarddiskVolume2\Users\target\Downloads\ticket.png
0x000000007fccbb20      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (6).png
0x000000007fccbe60      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (9).png
0x000000007fcd5b70      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (13).png
0x000000007fcd5df0      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (4).png
0x000000007fcdbf20      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (15).png
0x000000007fce4a30      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (10).png
0x000000007fce6350      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (19).png
0x000000007fedcca0      16      0 RW----
\Device\HarddiskVolume2\Users\target\Desktop\ticket - Copy (20).png
yakuhto@furry-catstation:~/ctf/unr2/hiddentypo$
```

Se pot observa mai multe imagini **png** în diferite locații. Dacă extragem una putem vedea flag-ul:

```
yakuhto@furry-catstation:~/ctf/unr2/hiddentypo$ volatility -f admin.bin
--profile=Win7SP1x64 dumpfiles -Q 0x000000007fc987d0 -D dump/ -u
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7fc987d0 None
\Device\HarddiskVolume2\Users\target\Desktop\ticket.png
yakuhto@furry-catstation:~/ctf/unr2/hiddentypo$ mv
dump/file.None.0xfffffa80317f5b0.dat ./image.png
yakuhto@furry-catstation:~/ctf/unr2/hiddentypo$ file image.png
image.png: PNG image data, 480 x 360, 8-bit/color RGB, non-interlaced
```



```
yakuhito@furry-catstation:~/ctf/unr2/hiddentypo$
```

Handwritten text in black ink on a white background. The text reads "Flag:" followed by "sha256" and a plus sign, and then "raw" on the next line.

Observație: Switch-ul **-u** din comanda de **dumpfiles** este foarte important. În multe situații, omiterea acestuia poate duce la inabilitatea programului **volatility** de a extrage unele fișiere.

Flag-ul este **ctf{sha256('flag')}**, adica **ctf{807d0fbcae7c4b20[redacted]6104122c5073e7744c46c4b87}**.

Rezolvare în engleză: <https://blog.kuhi.to/unbreakable-romania-2-writeup#hiddentypo>

## Not-clear (mediu - ridicat)

Concurs: UNbreakable #2 (2020)

Descriere:

```
I might be close to what you think.
```

```
Flag format: CTF{sha256}
```

Rezolvare:

Fișierul dat conține multe linii cu date aproape indescifrabile:

```
yakuhito@furry-catstation:~/ctf/unr2/notclear$ head -n 25
misc_not-clear_togive_not-clear.txt
+-----+-----+-----+
08:14:42,534,679    ETHER
|0
|ac|67|5d|71|cb|3b|e8|65|d4|ea|8e|20|08|00|45|00|00|37|00|00|40|00|3a|11|bc
|4c|ac|d9|13|6e|c0|a8|03|7a|01|bb|9b|0b|00|23|26|ee|45|a7|4e|18|cf|d6|86|fa
|1a|61|23|4e|23|87|e5|59|f8|37|f8|54|55|f3|45|14|11|d3|e9|

+-----+-----+-----+
08:14:42,534,679    ETHER
|0
|ac|67|5d|71|cb|3b|e8|65|d4|ea|8e|20|08|00|45|00|00|35|00|00|40|00|3a|11|bc
|4e|ac|d9|13|6e|c0|a8|03|7a|01|bb|9b|0b|00|21|86|dc|46|72|9e|cc|71|2f|30|24
|99|23|fd|2e|bf|1a|70|37|3f|e7|84|63|f9|84|73|97|da|

+-----+-----+-----+
08:14:42,539,549    ETHER
|0
|ac|67|5d|71|cb|3b|e8|65|d4|ea|8e|20|08|00|45|00|00|3c|00|00|40|00|3a|11|bb
|a7|ac|d9|14|0e|c0|a8|03|7a|01|bb|bc|e9|00|28|a2|2c|47|af|d3|c5|38|0a|4a|b7
|5b|38|84|6b|35|8d|9a|c3|3e|e1|71|a2|35|62|7c|80|56|aa|ce|ca|52|fb|f0|c0|

+-----+-----+-----+
08:14:42,548,603    ETHER
|0
|ac|67|5d|71|cb|3b|e8|65|d4|ea|8e|20|08|00|45|00|00|36|00|00|40|00|3a|11|bb
|ad|ac|d9|14|0e|c0|a8|03|7a|01|bb|bc|e9|00|22|af|67|53|d3|ba|ae|1b|73|a3|1e
|5f|05|aa|b0|8e|66|4b|43|0c|73|22|1a|ba|ec|45|9b|2d|0b|

+-----+-----+-----+
08:14:42,548,734    ETHER
|0
|e8|65|d4|ea|8e|20|ac|67|5d|71|cb|3b|08|00|45|00|00|3e|9d|54|40|00|40|11|18
|51|c0|a8|03|7a|ac|d9|14|0e|bc|e9|01|bb|00|2a|85|45|54|17|69|e4|31|17|c0|04
|67|56|ca|d9|d7|33|42|31|49|b6|da|20|99|32|e1|3d|72|02|ac|1a|f7|f4|00|e1|0d
|26|

+-----+-----+-----+
08:14:42,560,040    ETHER
```

```
|0  
|ac|67|5d|71|cb|3b|e8|65|d4|ea|8e|20|08|00|45|00|00|35|00|00|40|00|3a|11|bc  
|4e|ac|d9|13|6e|c0|a8|03|7a|01|bb|9b|0b|00|21|e7|15|52|17|e1|24|5d|a3|43|e0  
|b3|a0|d4|49|00|85|ae|a1|50|f0|7e|2f|21|f4|0d|80|ed|  
  
+-----+-----+-----+  
yakuhto@furry-catstation:~/ctf/unr2/notclear$
```

Cum exercitiul este incadrat in categoria **forensics** si fiecare set de date are **ETHER** pe prima linie, putem presupune ca datele date in format hex reprezinta continuturile unor pachete TCP sau UDP. Putem folosi [aceasta postare](#) pentru a face un script care sa transforme fișierul într-unul de tip **pcap**:

```
# import module  
import struct  
import time  
  
#      Pcap Global Header Format :  
#      ( magic number +  
#      major version number +  
#      minor version number +  
#      GMT to local correction +  
#      accuracy of timestamps +  
#      max length of captured #packets, in octets +  
#      data link type)  
#  
#  
  
PCAP_GLOBAL_HEADER_FMT = '@ I H H i I I I '  
  
# Global Header Values  
PCAP_MAGICAL_NUMBER = 2712847316  
PCAP_MJ_VERN_NUMBER = 2  
PCAP_MI_VERN_NUMBER = 4  
PCAP_LOCAL_CORECTIN = 0  
PCAP_ACCUR_TIMESTAMP = 0  
PCAP_MAX_LENGTH_CAP = 65535  
PCAP_DATA_LINK_TYPE = 1
```

```
class Pcap:

    def __init__(self, filename, link_type=PCAP_DATA_LINK_TYPE):
        self.pcap_file = open(filename, 'wb')
        self.pcap_file.write(struct.pack('@ I H H i I I I ', PCAP_MAGICAL_NUMBER,
PCAP_MJ_VERN_NUMBER, PCAP_MI_VERN_NUMBER, PCAP_LOCAL_CORRECTIN,
PCAP_ACCUR_TIMESTAMP, PCAP_MAX_LENGTH_CAP, link_type))
        print "[+] Link Type : {}".format(link_type)

    def writelist(self, data=[]):
        for i in data:
            self.write(i)
        return

    def write(self, data):
        ts_sec, ts_usec = map(int, str(time.time()).split('.'))
        length = len(data)
        self.pcap_file.write(struct.pack('@ I I I I ', ts_sec, ts_usec, length,
length))
        self.pcap_file.write(data)

    def close(self):
        self.pcap_file.close()

p = Pcap("a.pcap")
s = open("misc_not-clear_togive_not-clear.txt", "r").read().split("\n")
for i in s:
    if "|" not in i:
        continue
    packet = ''.join(i.split("|")[2:-1])
    p.write(packet.decode('hex'))
p.close()
```

După ce executam scriptul, putem deschide **pcap**-ul in **WireShark**. Pe langa multe pachete UDP, putem vedea și unele pachete TCP care fac parte dintr-o comunicare HTTP. Daca dam follow la unul dintre **HTTP POSTurile** din fișier, putem vedea flag-ul:



Rezolvare în engleză: <https://blog.kuhi.to/unbreakable-romania-2-writeup#notclear>

## Contribuitori

- Mihai Dancaesu (yakuhto)
- Andrei Avadanei