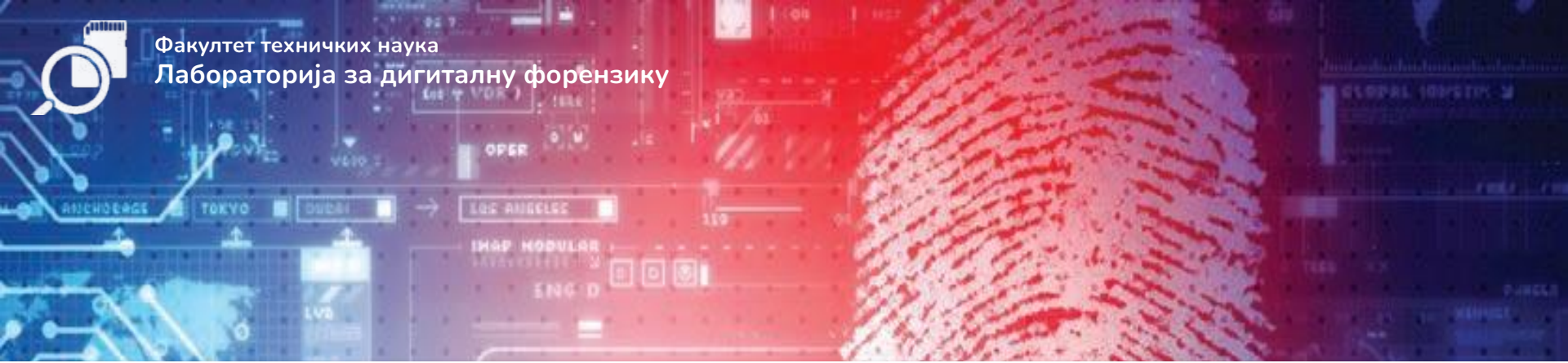


Факултет техничких наука
Лабораторија за дигиталну форензику

ФОРЕНЗИКА МАСОВНЕ МЕМОРИЈЕ

Увод у дигиталну форензику

Јелена Драгишић, Светлана Антешевић

Преглед области

Чиме се бави форензика масовне меморије?

Спада под област форензике рачунара.

Бави се дигиталним доказима који се налазе у интерним складиштима података (HDD, SSD) или у екстерним складиштима података (USB, DVD, CD, SD итд).

Ова складишта података представљају сталну (енг. non-volatile) меморију чије су битне карактеристике: капацитет, брзина приступа (читање, писање), цена.

Преглед области

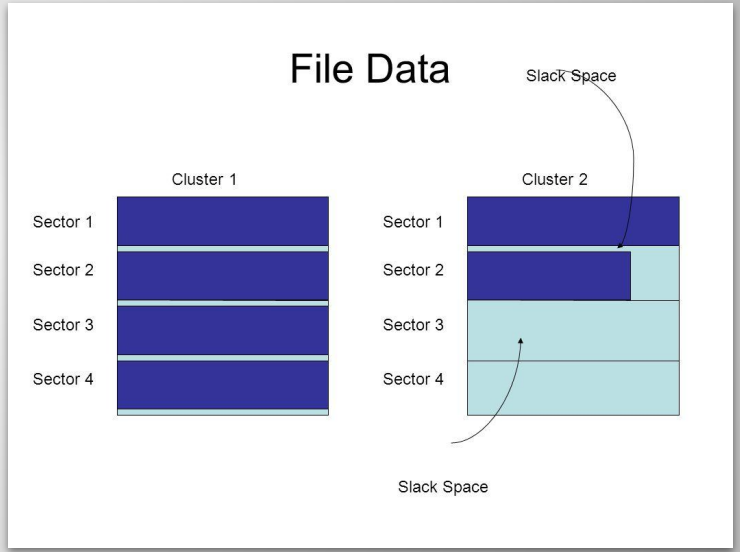
Који су типови складишта података?

1. По локацији
   a. Интерна (у рачунару)
   b. Екстерна (ван рачунара)
2. По технологији израде
   a. Електронска
   b. Магнетна
   c. Оптичка
3. По интерфејсу
   a. SATA
   b. SAS
   c. PCIe
   d. USB

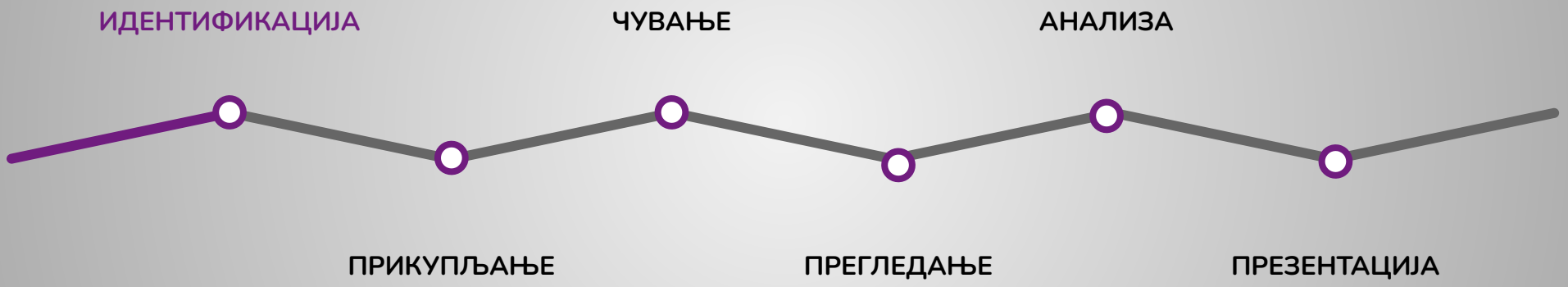
Преглед области

Шта представља изазов?

- ➔ Скривене и празне партиције
- ➔ Обрисане датотеке
- ➔ *Slack* простор
- ➔ Виртуелна меморија



Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

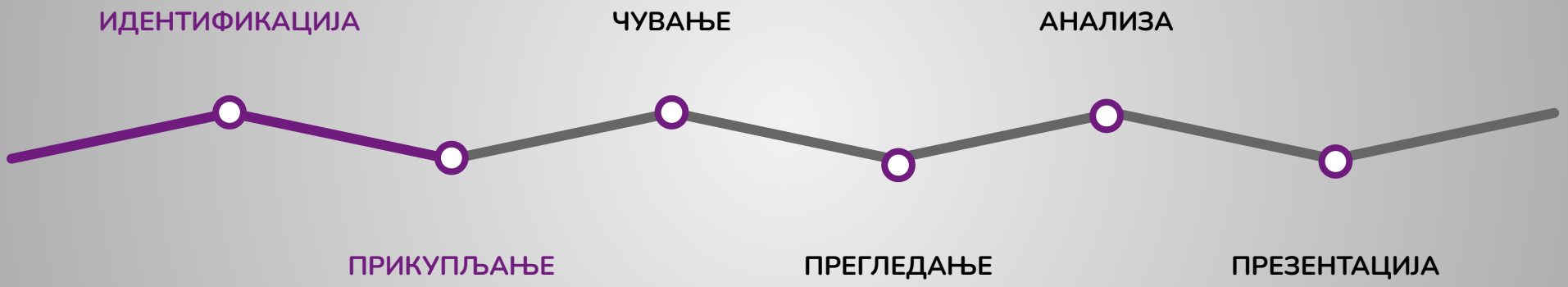
Идентификација

Односи се на детектовање, препознавање и одређивање дигиталних уређаја које треба истражити.

Под идентификацијом се подразумева и очитавање идентификатора дигиталних уређаја, који се истражују (произвођач, модел, серијски број).

Примери: рачунар, екстерни диск, USB стик, SD картица, документација о месту догађаја (фотографије, видео снимци, гласовни снимак), просторија у којој се налази уређај, стање уређаја, књиге, белешке, каблови...

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Прикупљање

Идентификоване доказе је потребно прикупити коришћењем научно и правно ваљаних метода.

Прављење форензичке копије HDD, SSD, USB...

Потребно је припремити медије на којима се прави форензичка копија.

Потребна опрема:

- ➔ Блокатори писања (хардверски и софтверски)
- ➔ Читачи картица
- ➔ Каблови и адаптери

Прикупљање помоћу форензичког дупликатора

Tableau TX1

Преносиви форензички дупликатор.

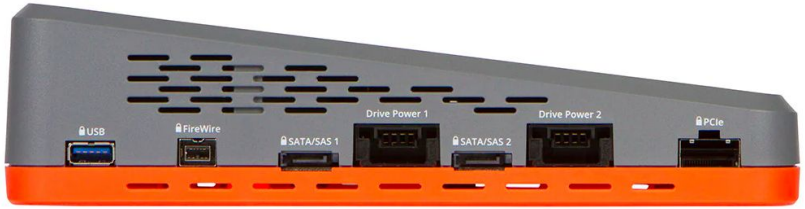
- ➔ Врши бит по бит копију података са складишта података.
- ➔ Логичка копија складишта података.
- ➔ Сигурно брисање дискова.
- ➔ Подржава прављење две копије података.
- ➔ Подржава различите интерфејсе (SATA, SAS, USB).

Прикупљање помоћу форензичког дупликатора

Tableau TX1 - кораци

1. Повезати изворно складиште података на одговарајући интерфејс.
2. Повезати одредишно складиште података на одговарајући интерфејс.

1.

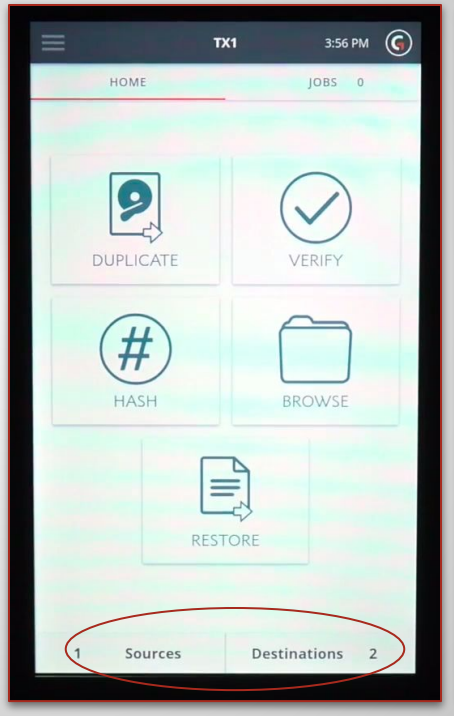


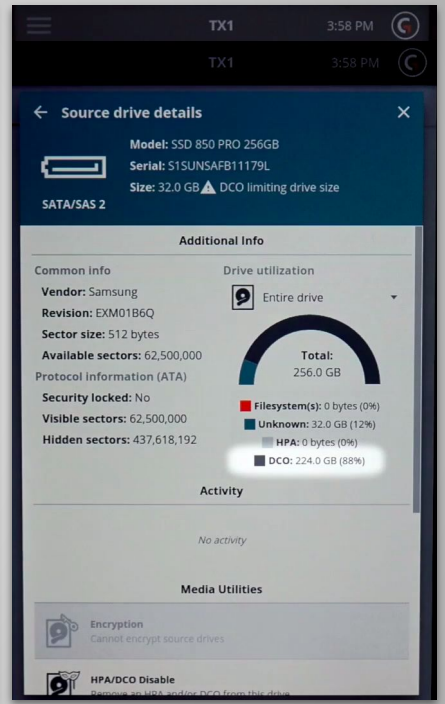
2.

Прикупљање помоћу форензичког дупликатора

Tableau TX1 - кораци

3. Укључити уређај
4. Након препознавања изворног и одредишног уређаја, постоји могућност увида у детаље о њима (опције *source* и *destination* на дну екрана).

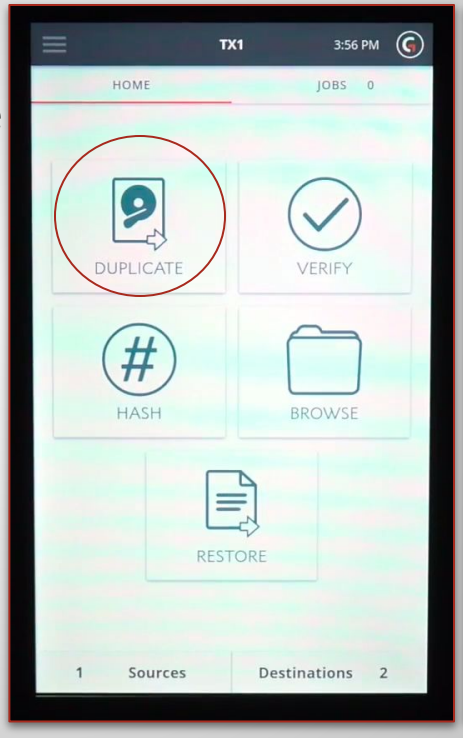


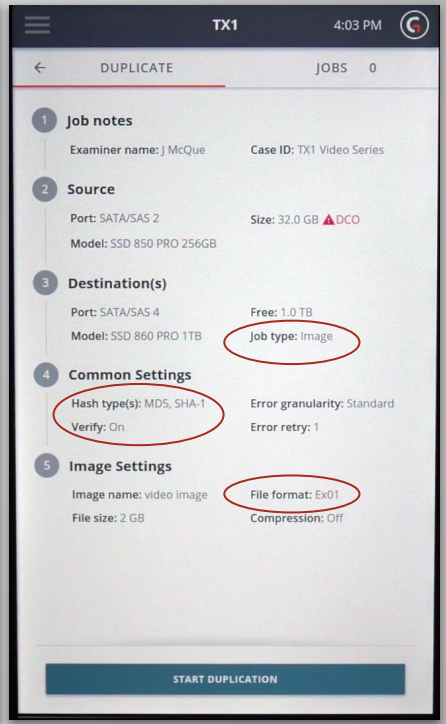


Прикупљање помоћу форензичког дупликатора

Tableau TX1 - кораци

5. За прављење форензичке копије потребно је одабрати опцију *duplicate*.
6. Подесити опције: селектовати изворни и одредишне уређаје, подесити формате слике и хеш алгоритме.
7. Покренути прављење форензичке копије кликом на дугме *start duplication*.

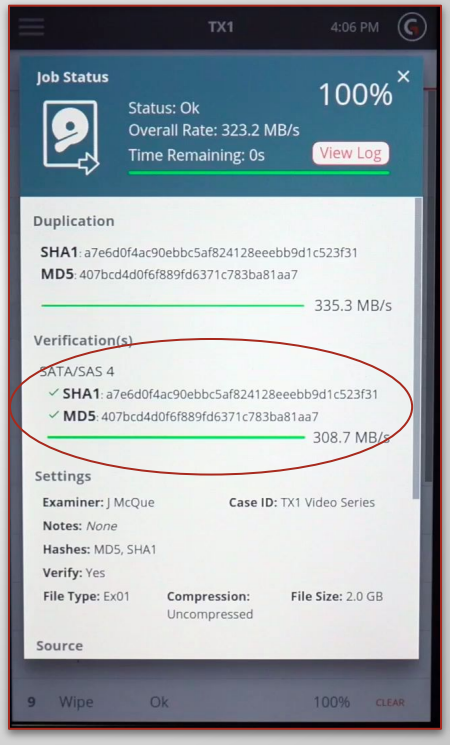


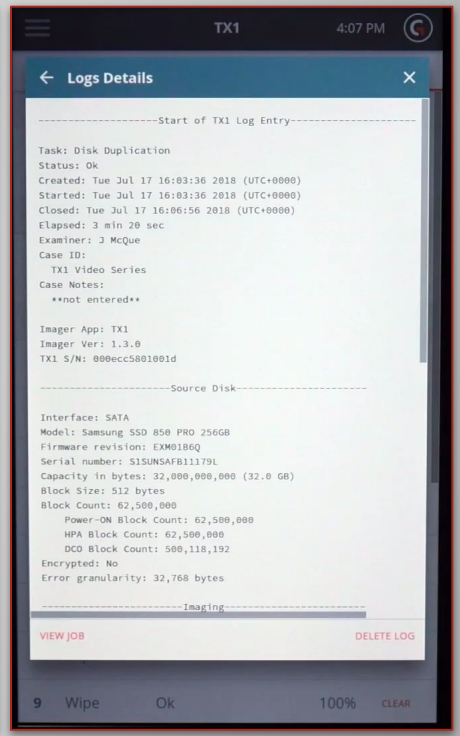


Прикупљање помоћу форензичког дупликатора

Tableau TX1 - кораци

8. Прављење форензичке копије може потрајати у зависности од количине података.
9. На крају прављења копије могуће је сачувати лог на складиште података.





Прикупљање помоћу Data Dump (dd) алата

Data Dump (dd)

Програм командне линије за Unix оперативне системе.

Користи се за:

- ➔ Прикупљање или клонирање података са диска у *bitstream* (необрађеном) формату
- ➔ Копирање партиција диска
- ➔ Копирање фолдера и датотека
- ➔ Провера грешки на хард диску
- ➔ Брисање свих података са хард диска

Прикупљање помоћу Data Dump (dd) алата

Препознавање диска и партиција на диску помоћу **fdisk** команде:

$ [sudo] fdisk -l

Рачунање хеш вредности диска како бисмо се уверили да је форензичка копија правилно направљена.

➔ MD5 алгоритам: **$ [sudo] md5sum [disk path]**
➔ SHA1 алгоритам: **$ [sudo] sha1sum [disk path]**

Прикупљање помоћу Data Dump (dd) алата

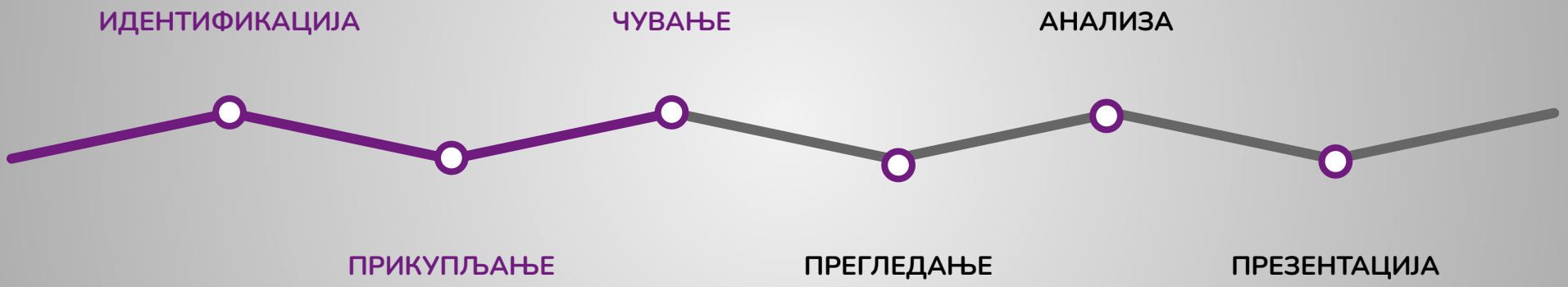
Прављење форензичке копије помоћу dd алата:

$ [sudo] dd if=/dev/sdb of=sdb_image.img bs=512 conv=noerror,sync

$ [sudo] dd if=/dev/sdb bs=512 conv=sync,noerror | split -d -b 650m - sdb_image.

- ➔ **if** : путања где се налази диск
- ➔ **of** : путања и назив одредишне копије диска са одговарајућом екстензијом
- ➔ **bs** : величина блока (512 је подразумевано) [опционо]
- ➔ **conv** : конверзија (noerror - наставиће да се извршава и када наиђе на грешку; sync - ако постоји грешка неће попунити остатак блока) [опционо]
- ➔ **split** : подела одредишне копије диска на више датотека (d - нумерички редослед, b - величина датотека) [опционо]

Процес форензичке истраге



Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Чување

Прикупљени докази морају се сачувати коришћењем физичких, техничких и организационих контрола.

Верификација копије диска помоћу рачунања хеш вредности (са неким од алгоритама: sha1, sha256, md5) да би се обезбедио интегритет доказа. Команда за рачунање у току прикупљања:

$ dd if=/dev/sdb bs=512 conv=sync,noerror | tee sdb_image.img | md5sum > sdb_image.md5

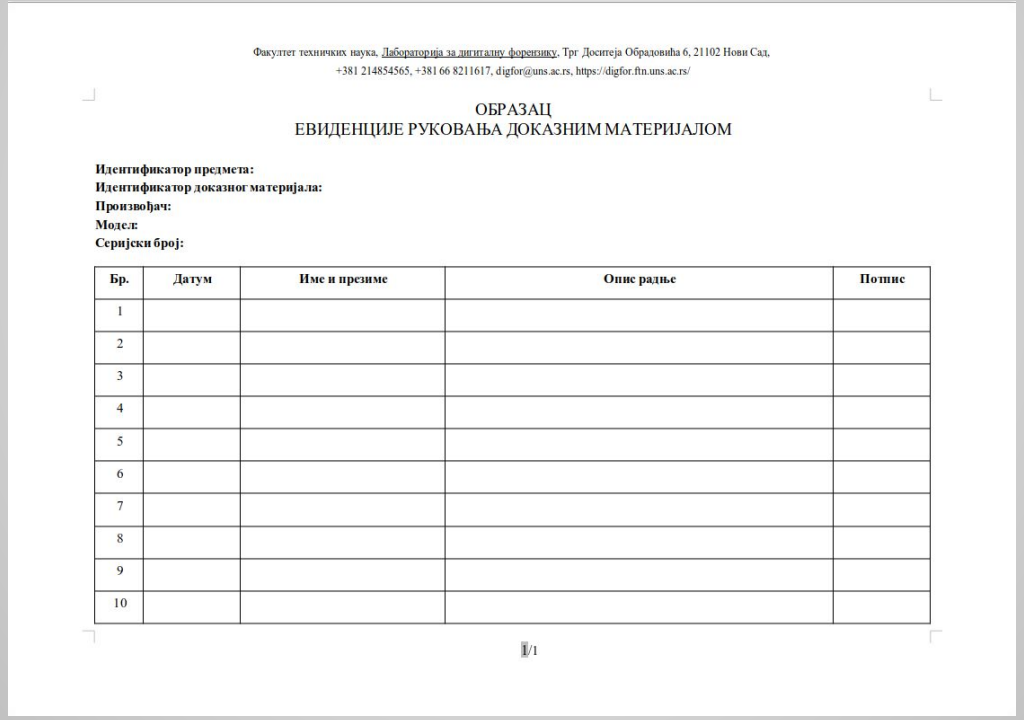
Рачунање хеш вредности након копирања:

$ md5sum /tmp/sdb_image.img> /tmp/image-md5

$ cat sdb_image.* | md5sum >> md5_sdb.txt

Чување

Ланац доказа - евиденција о томе када и ко је имао приступ доказима.



Факултет техничких наука, Лабораторија за дигиталну форензику, Трг Доситеја Обрадовића 6, 21102 Нови Сад,
+381 214854565, +381 66 8211617, digfor@uns.ac.rs, https://digfor.ftn.uns.ac.rs/

ОБРАЗАЦ
ЕВИДЕНЦИЈЕ РУКОВАЊА ДОКАЗНИМ МАТЕРИЈАЛОМ

Идентификатор предмета:
Идентификатор доказног материјала:
Произвођач:
Модел:
Серијски број:

Бр.	Датум	Име и презиме	Опис радње	Потпис
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

1/1

Чување

Докази се чувају у одговарајућем формату датотека који омогућавају компресију података, поделу датотека на више датотека и шифровање датотека.

- ➔ E01 - власнички формат датотека (EnCase)
- ➔ AFF - отворени формат датотека (Autopsy)
- ➔ DD, IMG, RAW, BIN - сирови формати датотека
- ➔ VMDK, VDH - формати виртуелних машина

Процес форензичке истраге

Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Сценарио за анализу

- ➔ Полиција је запленила лаптоп особе, која је планирала оружани напад.
- ➔ Слика масовне меморије датог лаптопа направљена је помоћу алата FTK Imager.

Извор: https://digitalcorpora.org/corpora/scenarios/2018-lone-wolf-scenario

Прегледање и анализа

Autopsy & The Sleuth Kit

- ➔ The Sleuth Kit - скуп CLI алата за дигиталну форензику.
- ➔ Autopsy - GUI програм за The Sleuth Kit.
- ➔ Отвореног изворног кода.
- ➔ Прегледање и анализа и укључених и искључених рачунара.
- ➔ Дизајниран модуларно.

Прегледање и анализа

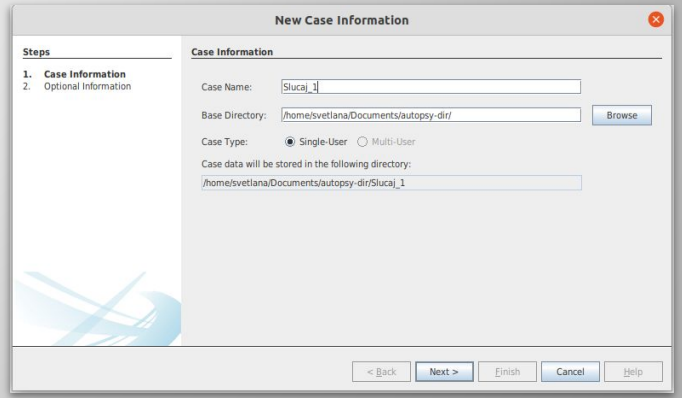
Autopsy & The Sleuth Kit:

1. Покренути Autopsy

   $ cd /opt/autopsy-4.19.2/bin

   $ ./autopsy

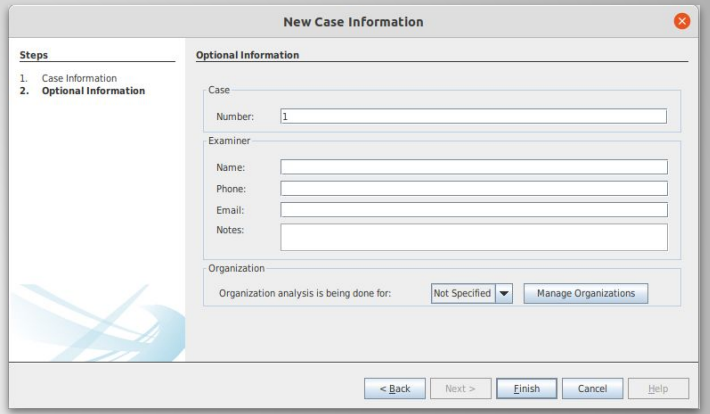
2. Направити нови случај, опција New Case или отворити постојећи, опција Open Recent Case или Open Case
3. Додати основне информације о случају (назив, одредишни фолдер).

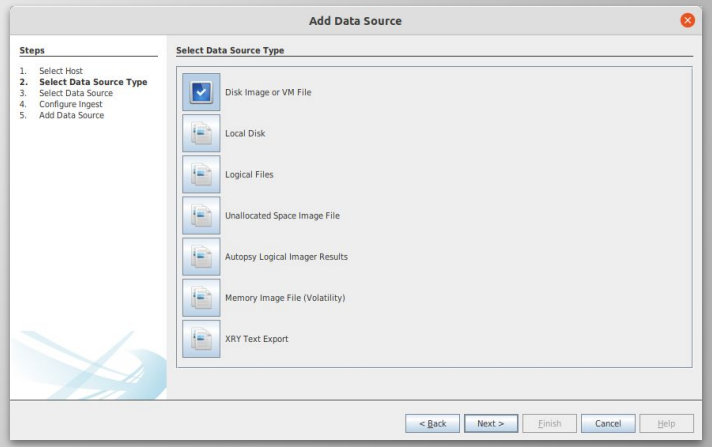


Прегледање и анализа

Autopsy & The Sleuth Kit – кораци:

4. Додати опционе податке о случају (број случаја, назив истражитеља, мејл, подаци о организацији...)
5. Одабрати Finish опцију како би се креирао нови случај.
6. Додати изворе података
   a. Disk image or VM file
   b. Logical disk
   c. Logical files
   d. Unallocated space image file
   e. Autopsy logical imager results
   f. Memory image file (volatility)
   g. XRY text export





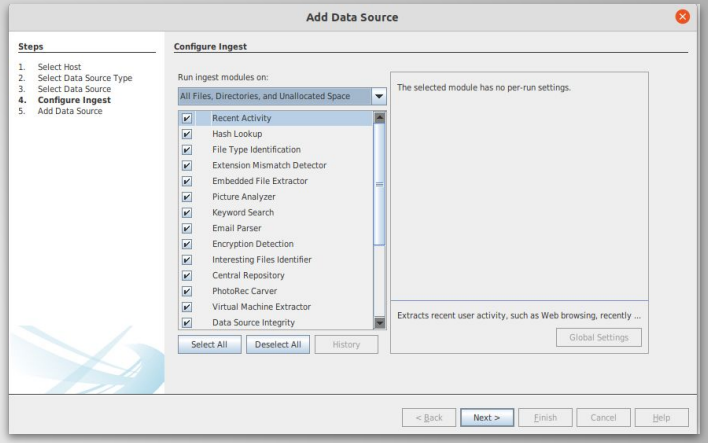
Прегледање и анализа

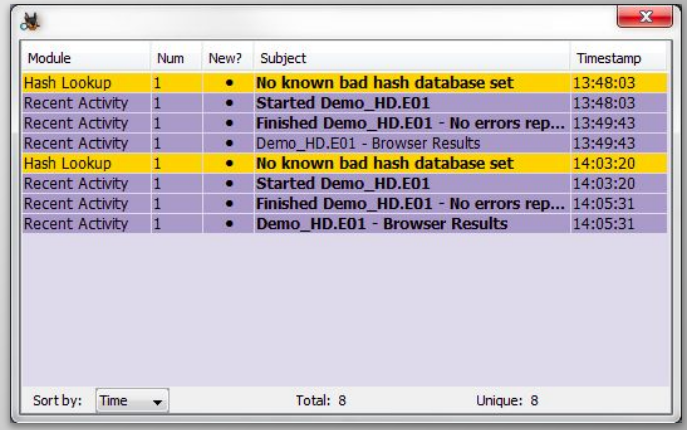
Autopsy & The Sleuth Kit – кораци:

7. Одабир ingest модула - они анализирају датотеке одмах након додавања извора података (могуће је и додати нове модуле).

   Сваки модул је могуће додатно исконфигурисати у табели са десне стране.

   Резултате ingest модула могуће је видети у порукама у горњем десном углу.





Прегледање и анализа

Autopsy ingest модули:

- **Recent Activity** - издваја корисничку активност у последњих 7 дана коју чувају веб претраживачи, инсталирани програми и оперативни систем.
- **Hash Lookup** - проверава да ли се у бази података са hash вредностима малициозних датотека налази нека од датотека из изворног медијума. Могуће је додатно исконфигурисати овај модул и проширити базу са hash вредностима.
- **File Type Identification** - идентификује датотеке на основу њихових интерних потписа и не ослања се на екстензије датотека. Многи модули зависе од резултата овог модула.
- **Extension Mismatch Detector** - користи се да идентификује неусклађеност екстензија и типа датотеке. Овај модул открива датотеке које неко можда покушава да сакрије.
- **Keyword Search** - модул за претрагу кључних речи олакшава пертраживање тако што извлачи текст из подржаних формата датотека и смешта у Solr index који се касније може претраживати. Испоручује се са већ неким уграђеним листама које дефинишу регуларне изразе и омогућавају кориснку да тражи бројеве телефона, IP адресе, URL адресе, адресе е-поште.

Прегледање и анализа

Autopsy ingest модули:

- **Embedded File Extractor** - отвара архивске датотеке ZIP, RAR и друге формате као што су doc, docx, ppt, xls, xlsx како би омогућио анализу ових датотека (претрагу кључних речи, тражење hash-a).
- **Picture Analyzer** - овај модул издваја Exchangeable Image File Format (EXIF) информације из слика тј. метаподатке.
- **Email Parser** - идентификује Thunderbird MBOX датотеке и PST формате датотека на основу потписа датотека, издваја е-поруке из њих, додаје прилоге као изведене датотеке.
- **Encryption Detection** - овај модул детектује датотеке над којима је примењен неки алгоритам за криптовање.
- **Interesting Files Identifier** - омогућује да се претражују датотеке или директоријуми у извору података и генерише упозорења када се пронађу. Могуће је конфигурисати модул да даје обавештења када се пронађу одређене ствари.
- **Central Repository** - Централно спремиште омогућава кориснику да пронађе артефакте који се подударају у свим случајевима и у различитим изворима података у истом случају.
- **PhotoREc Carver** - издваја датотеке из недодељеног простора у извору података и приказује пронађене датотеке.

Прегледање и анализа

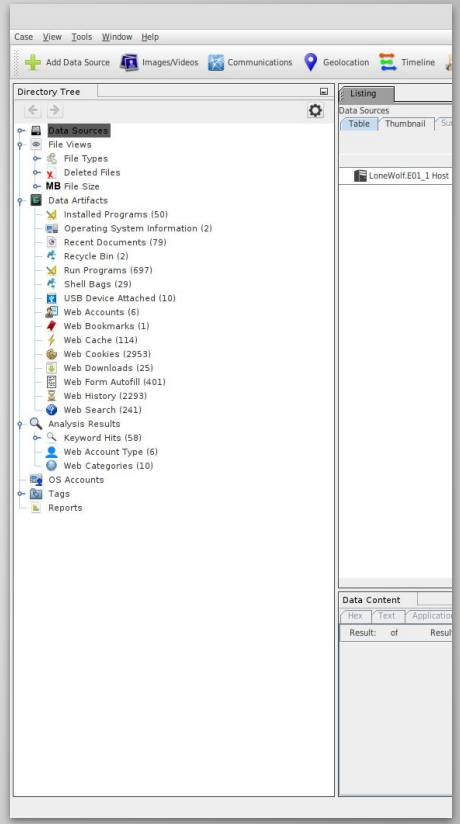
Autopsy ingest модули:

- **Virtual Machine Extractor** - додаје све виртуелне машине које пронађе у извору података у случај као нове изворе података.
- **Data Source Integrity** - Ако извор података има било какве хешове повезане са њим (било које је унео корисник или садржане у E01 датотеци), он ће верификовати ове хешове или ако извор података нема придружене хешове, он ће израчунати хешове и сачувати их у бази података.
- **Android Analyzer (aLEAPP)** - омогућава да се анализирају датотеке са Android уређаја.
- **DJI Drone Analyzer** - анализира датотеке са дрона.
- **Object Detection** - користи OpenCV да детектује објекте на сликама.
- **Plaso -** издваја временске ознаке (timestamps) из различитих типова датотека.
- **YARA Analyzer -** је дизајнирана за анализу злонамерног софтвера, али се може користити за претрагу било које врсте датотека.
- **iOS Analyzer (iLEAPP)** - омогућава да се анализирају датотеке са iOS уређаја.
- **GPX Parser** - омогућава да се увезу GPS подаци из GPX фајлова.

Прегледање и анализа

Autopsy & The Sleuth Kit – кораци:

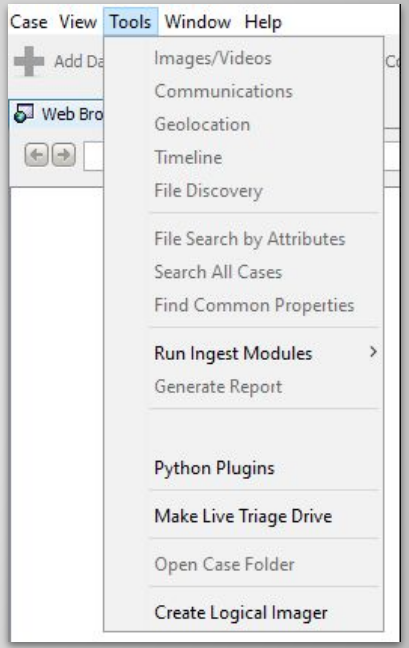
8. Покренути анализу. Може потрајати неко време у зависности од количине података и одабраних модула.
9. Са леве стране може се видети стабло са подацима о извору података (Data Source), преглед података по типу (File Views), пронађени подаци у зависности од означених модула (Data Artifacts), обрисане датотеке, шифроване датотеке итд.

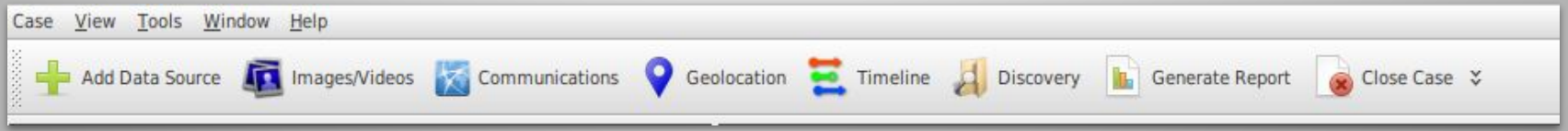


Прегледање и анализа

Autopsy & The Sleuth Kit – кораци:

10. Могуће је додати више извора података одабиром опције Add Data Source.
11. У картици Tools постоје додатни алати за анализу података.

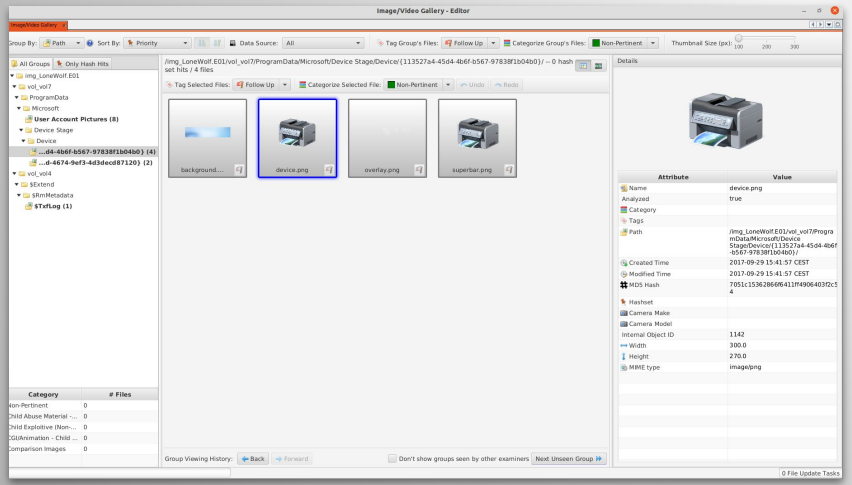


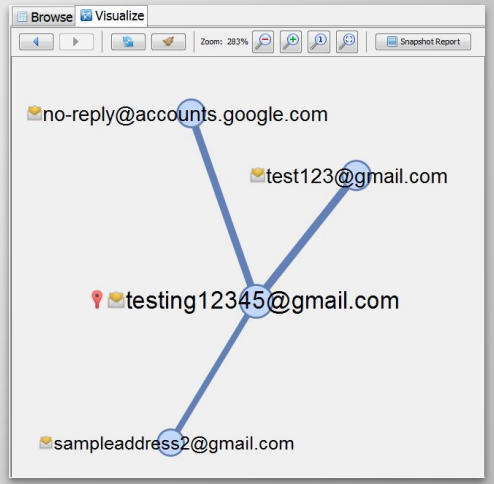


Прегледање и анализа

Autopsy & The Sleuth Kit – кораци:

12. Алат за анализу мултимедијалних података: фотографија, видео записа и њихових метаподатака.
13. Алат за анализу комуникација на основу пронађених мејл комуникација. Може да визуализује комуникацију.

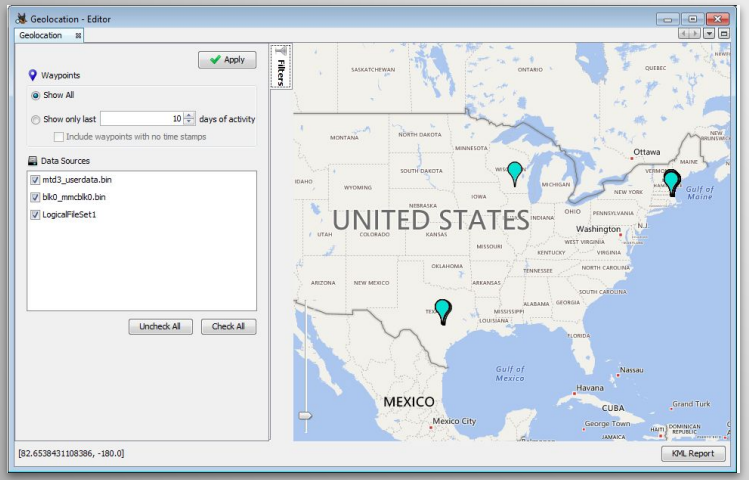


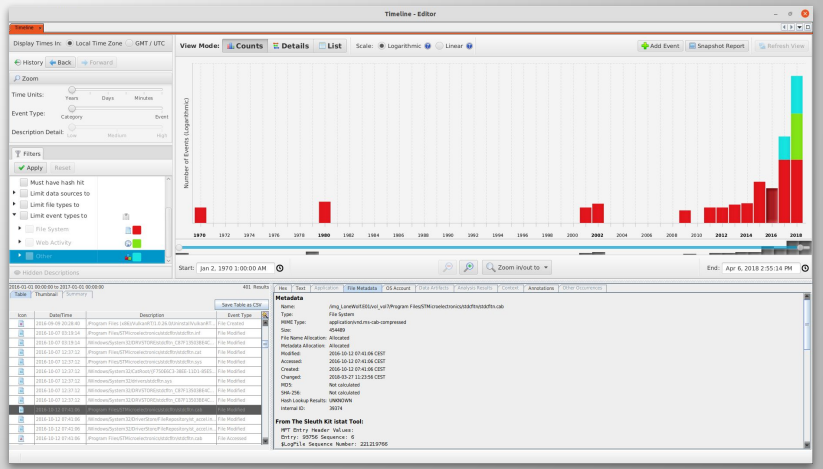


Прегледање и анализа

Autopsy & The Sleuth Kit – кораци:

14. Алат за анализу локација на основу података о географској ширини и дужини
15. Алат за анализу временских информација о подацима.

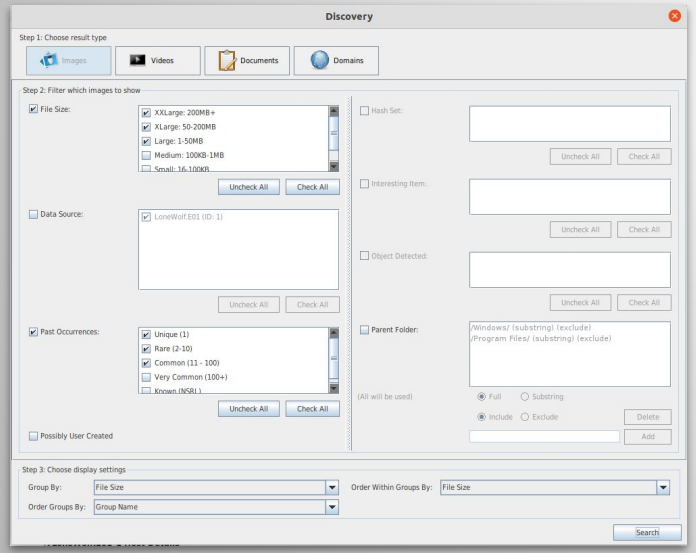


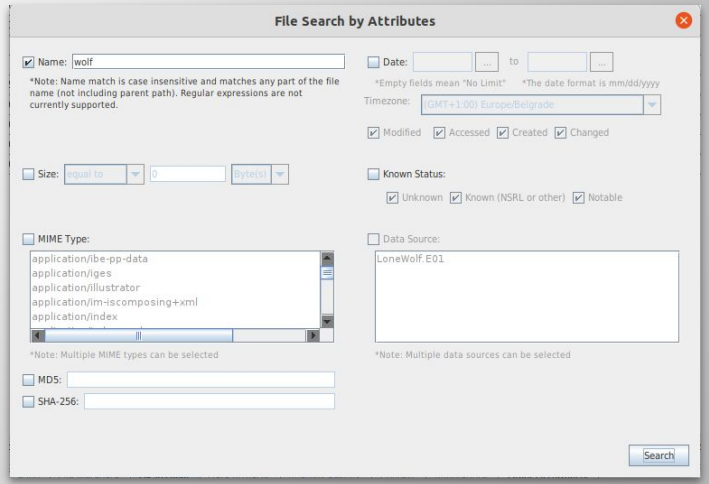


Прегледање и анализа

Autopsy & The Sleuth Kit – кораци:

16. Алати за напредне претраге по одређеним метаподацима фајлова, задатим речима, типовима докумената, хеш вредносима...





Прегледање и анализа

Foremost

- ➔ Форензички програм за опоравак изгубљених датотека на основу њихових заглавља, подножја и интерних структура података.
- ➔ Може да ради на датотекама слика, као што су оне које генерише dd, Safeback, Encase, итд или директно на диску.

Прегледање и анализа

Foremost

$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>] [-b <size>] [-c <file>] [-o <dir>] [-i <file]

- -V - приказ информација о ауторским правима и излаз.
- -t - наведите тип датотеке (-t jpeg,pdf ...).
- -d - укључи индиректну детекцију блока (for UNIX file-systems).
- -i - наведите улазну датотеку (default is stdin).
- -a - Напишите сва заглавља, не откривајте грешке (оштећене датотеке).
- -w - Запишите само датотеку ревизије, немојте писати ниједну откривену датотеку на диск.
- -o - постави излазни директоријум (defaults to output).
- -c - подесите конфигурациону датотеку за употребу (defaults to foremost.conf).
- -q - омогућава брзи режим. Претрага се врши на границама од 512 бајтова.
- -Q - омогућава тихи режим. Потисните излазне поруке.
- -v - опширни начин (verbose mode). Евидентира све поруке на екрану.

Прегледање и анализа

Foremost

$ foremost -t doc,jpg,pdf,xls -i image.dd -o /output

```
└─$ foremost -t pdf -o /home/kali/LDF/nesto -i paja_ram.raw -v
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Mar  3 23:09:07 2023
Invocation: foremost -t pdf -o /home/kali/LDF/nesto -i paja_ram.raw -v
Output directory: /home/kali/LDF/nesto
Configuration file: /etc/foremost.conf
Processing: paja_ram.raw
|------------------------------------------------------------------
File: paja_ram.raw
Start: Fri Mar  3 23:09:07 2023
Length: 3 GB (4294500446 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

*******************************0:       06380713.pdf           2 KB      3266925364
**********|
Finish: Fri Mar  3 23:09:16 2023

1 FILES EXTRACTED

pdf:= 1
------------------------------------------------------------------

Foremost finished at Fri Mar  3 23:09:16 2023
```

Процес форензичке истраге

Напомена – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

Презентација

Резултати анализе доказа се презентују у писменом облику.

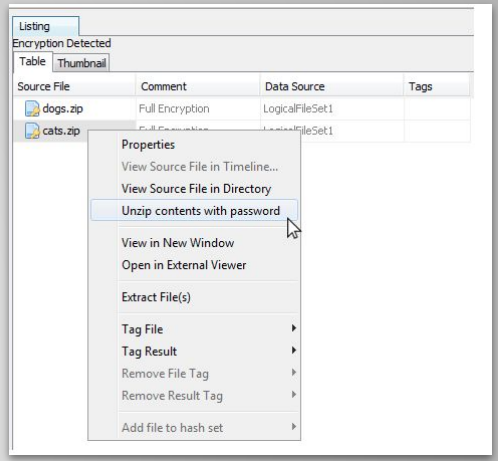
Односи се на процес којим форензичар дели резултате фазе анализе у облику извештаја заинтересованим странама.

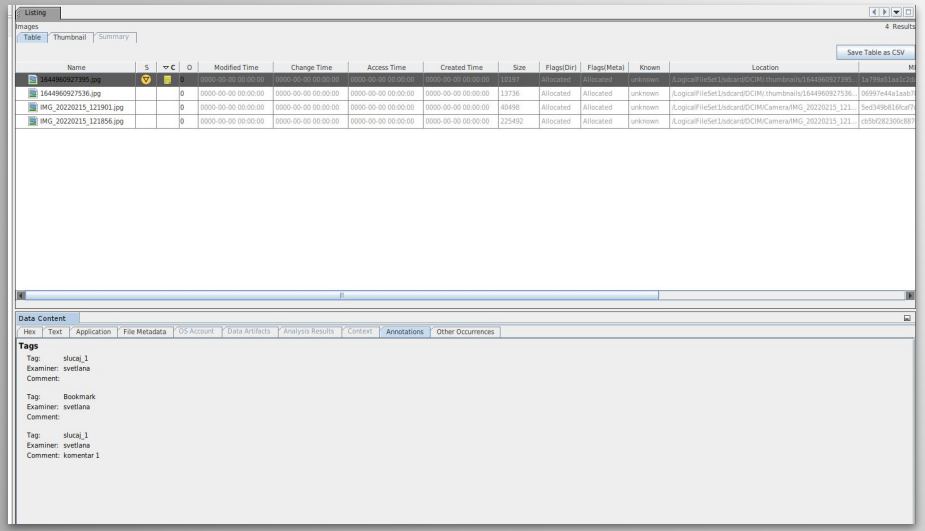
Форензичар обично сачињава налаз и мишљење и усмено га брани одговарајући на питања на главном судском претресу.

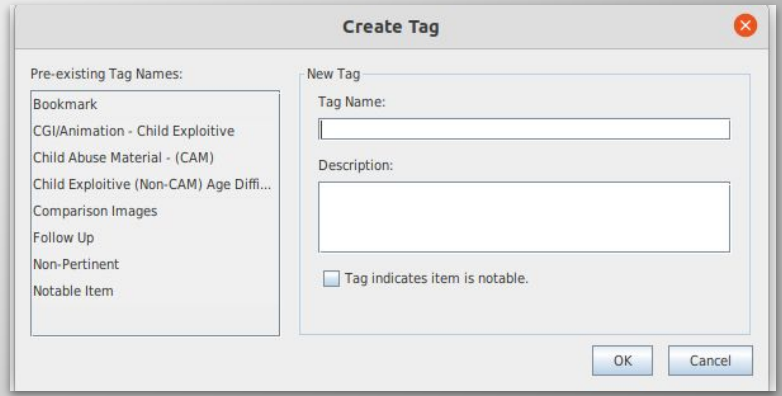
Презентација

Autopsy & The Sleuth Kit

- Све пронађене фајлове могуће је таговати са таг ознакама.
- Могуће је извести пронађене фајлове.



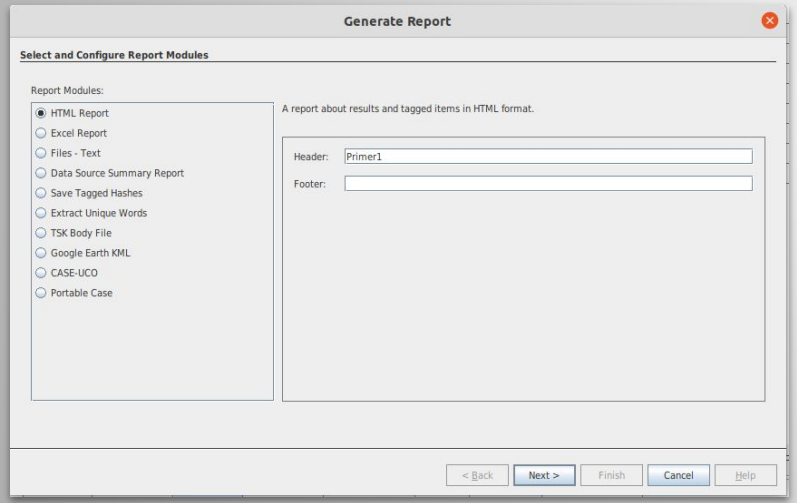


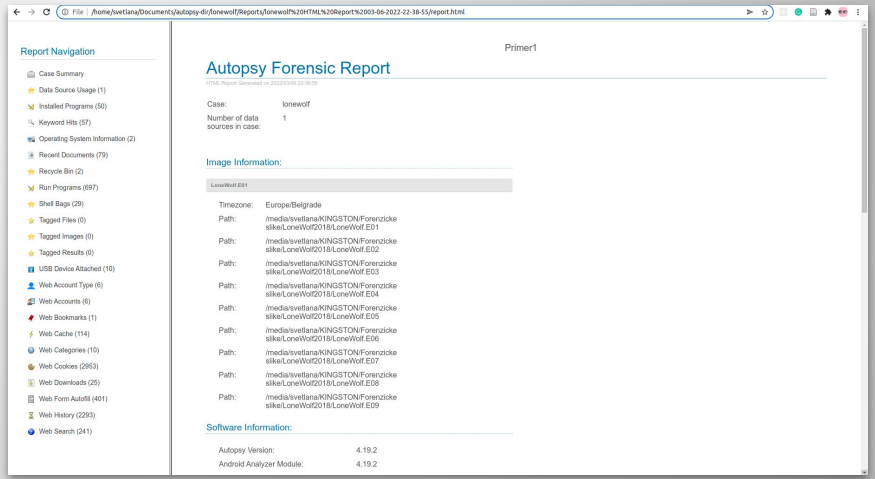


Презентација

Autopsy & The Sleuth Kit

Алат за генерисање извештаја у различитим форматима на основу тагованих и пронађених фајлова (опција Generate Report)





Корисни линкови и книге

- https://www.kali.org/docs/
- http://sleuthkit.org/autopsy/docs/user-docs/4.19.2/
- https://www.kali.org/tools/foremost/
- https://digitalcorpora.org/
- *Digital Forensics with Kali Linux*
- *Digital forensics : an academic introduction*