Факултет техничких наука
Лабораторија за дигиталну форензику

# ФОРЕНЗИКА ОПЕРАТИВНХ СИСТЕМА

Увод у дигиталну форензику

Јелена Драгишић, Светлана Антешевић

# Преглед области

**Чиме се бави форензика оперативних система?**

– Дигиталним доказима, који су резултат рада оперативног система.

**Којим артифактима рада оперативног система се бавимо?**

– Конфигурационим параметрима оперативног система.
– Логовима активности оперативног система.
– Конфигурационим параметрима корисника
– Логовима активности корисника.

# Преглед области

**Којим оперативним системима се бавимо?**

– Windows
– Linux

# Форензика оперативног система Windows

## Складишта артифаката оперативног система Windows

– Регистар
– Логови системске активности
– Логови најфреквентније коришћених апликација

# Форензика оперативног система Linux

## Артифакти оперативног система Linux

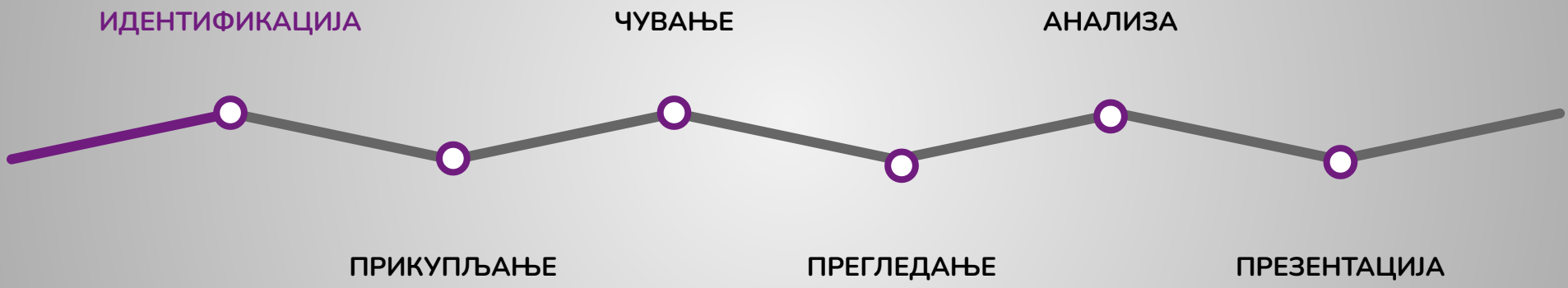
– Системске конфигурационе датотеке

– Кориснички специфична конфигурација

– Логови системске активности

– Логови корисничке активности

# Процес форензичке истраге




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

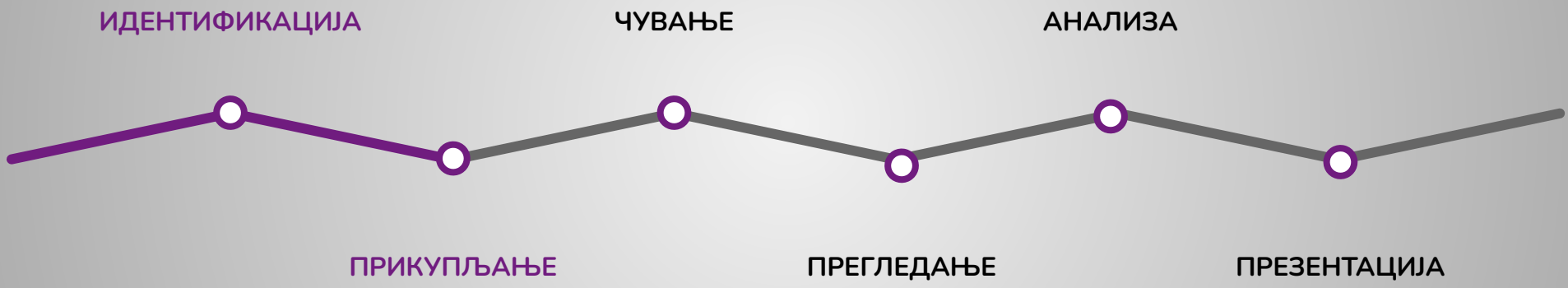
# Идентификација

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, документација о месту догађаја (фотографије, видео снимци, гласовни снимак), просторија у којој се налази уређај, стање уређаја, књиге, белешке, каблови...

# Процес форензичке истраге

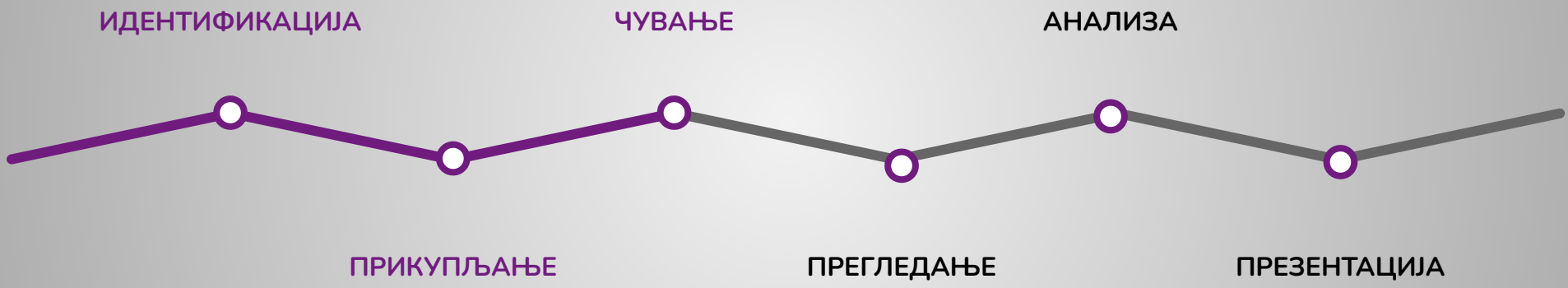



**Напомена** – етапе форензичке истраге не одвијају се секвенцијално. Често су репетитивне.

# Прикупљање

Креирање форензичке копије масовне меморије користећи хардверски уређај као што је форензички дупликатор и блокатор писања Tableau TX1 или софтверски алат као што су Data Dump (dd), FTK Imager и други (обрађено у претходном термину форензике масовне меморије).

# 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.

Рачунање хеш вредности у току прикупљања:

**$ dd if=/dev/sdb bs=65536 conv=sync,noerror | tee sdb_image.img | md5sum > sdb_image.md5**

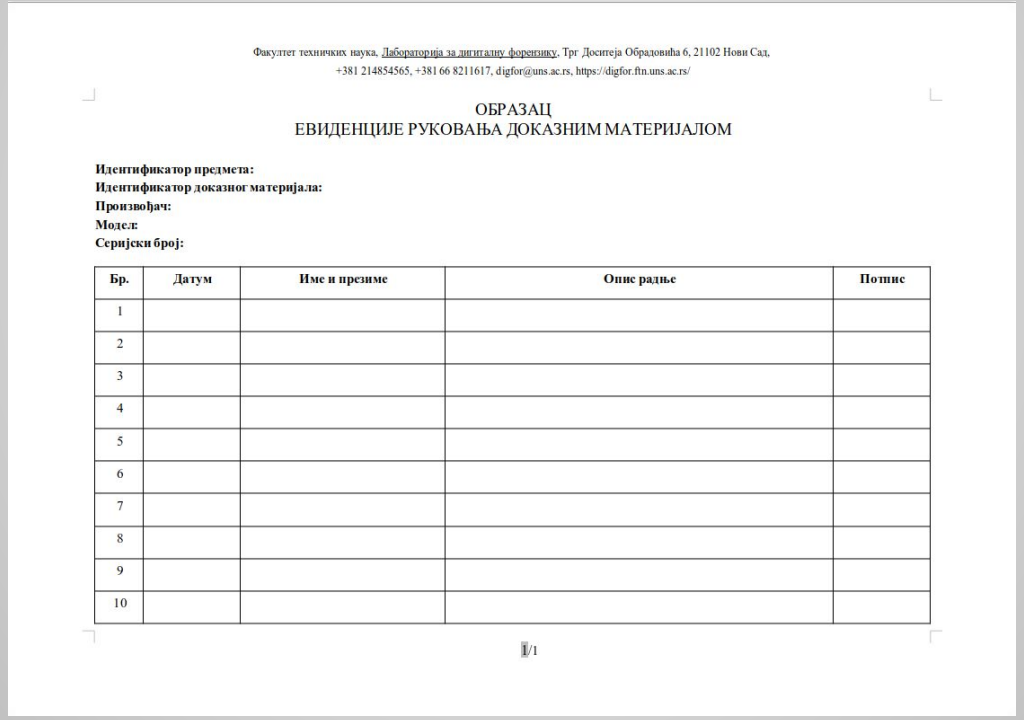
Рачунање хеш вредности након копирања:

**$ 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

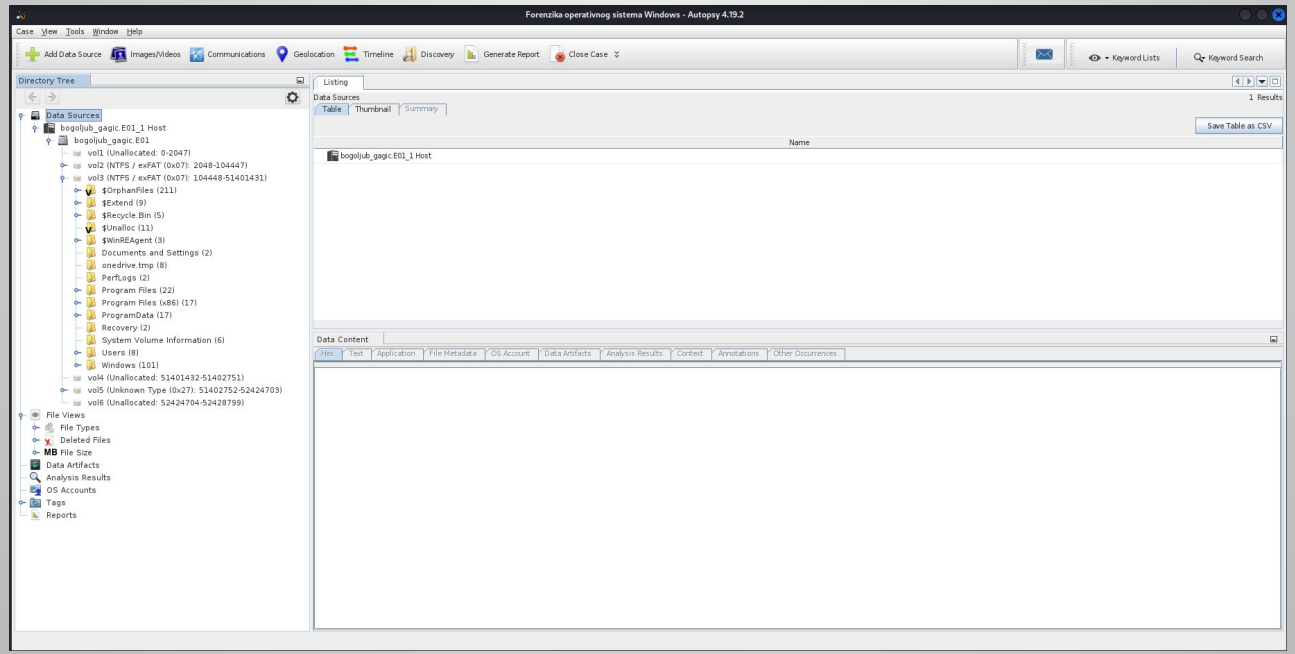
# Процес форензичке истраге


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

# Windows
(10)

# Прегледање артифаката оперативног система Windows

Увид у форензичку копију масовне меморије помоћу алата као што су Autopsy, FTK Imager итд.




Форензичка копија масовне меморије којом управља оперативни систем Windows 10 увезена у алат Autopsy

# Прегледање артифаката оперативног система Windows

Да би се омогућила анализа артифаката оперативног система Windows, потребно је помоћу одговарајућег алата (нпр. Autopsy) извести директоријуме који их садрже.

- Директоријуми који садрже кошнице регистра су **\Windows\System32\config** и **\Users\[корисничко име]**.
- Директоријум који садржи логове системске активности је **\Windows\System32\winevt\Logs**.
- Директоријум који садржи логове најфреквентније коришћених апликација је **\Windows\Prefetch**.

# Процес форензичке истраге


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

# Анализа артифаката оперативног система Windows

Алат који се најчешће користи за анализу артифаката оперативног система Windows је **RegRipper**.

Алат RegRipper представља парсер датотека са кошницама регистра. Типови датотека са кошницама које може да парсира су SAM (Security Accounts Manager), SECURITY, SYSTEM, SOFTWARE и NTUSER.DAT.

Кошнице SAM, SECURITY, SYSTEM и SOFTWARE складиште се у оквиру директоријума \Windows\System32\config\, док се датотека NTUSER.DAT налази у оквиру директоријума \Users\[корисничко име]\

# Анализа артифаката оперативног система Windows

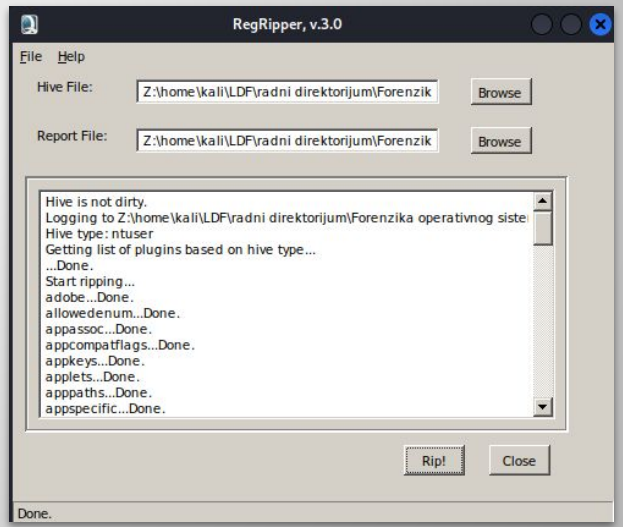
| Назив датотеке | Кошница | Опис |
|---|---|---|
| SOFTWARE | HKEY_LOCAL_MACHINE\SOFTWARE | Информације о инсталираним програмима, параметрима система у вези са перформансама, системска конфигурација |
| SYSTEM | HKEY_LOCAL_MACHINE\SYSTEM | Информације о хардверским компонентама (прикљученим уређајима) |
| SAM | HKEY_LOCAL_MACHINE\SAM | Информације о сервису за безбедно управљање налозима |
| SECURITY | HKEY_LOCAL_MACHINE\SECURITY | Информације о безбедности |
| NTUSER.DAT | HKEY_CURRENT_USER | Информације о активности корисника |

# Анализа артифаката оперативног система Windows

- Алат RegRipper чине скрипта писана у програмском језику *perl* и, у зависности од типа кошнице која се анализира, примењују се различита скрипта (енг. *plugins*).
- Графички кориснички интерфејс алата RegRipper приказан је на слици испод.
- Покретање:

```
$ cd /opt/RegRipper3.0/

$ wine rr.exe
```



# Анализа артифаката оперативног система Windows

- ➔ У поље означено лабелом ***Hive File*** потребно је унети путању до директоријума који представља кошницу регистра, док је у поље означено лабелом ***Report File*** потребно унети путању до текстуалне датотеке у коју ће се записати логови након што се скрипта RegRipper-а изврше.
- ➔ Програм је способан да на основу садржаја одабране кошнице одреди њен тип на основу кога ће се извршити одговарајућа скрипта.

# Анализа артифаката оперативног система Windows

Употреба алата RegRipper кроз командну линију:

Излиставање свих модула:

```
$ perl rip.pl.linux -l
```

Примена модула над кошницом

$ perl rip.pl.linux -r /путања_до_кошнице/датотека_кошнице -p назив_модула

Примена модула nic2 над датотеком са кошницама System

$ perl rip.pl.linux -r /home/kali/LDF/radni_direktorijum/vezbe3/Export/110783-SYSTEM -p nic2

# Анализа артифаката оперативног система Windows

Скрипта алата RegRipper могу се груписати у неколико категорија:

– скрипта која дају опште информације о оперативном систему (winnt_cv, producttype, win_cv, timezone, shutdown, shutdowncount, polacdms, winlogon, uac, disablesr, diag_sr, spp_clients, backuprestore, winbackup, bitbucket, disablelastaccess, dfrg, secctr, pagefile, hibernate, processor_architecture, crashcontrol, regback, ctrlpnl, banner, nolmhash, susclient, gpohist)

– скрипта која дају информације о налогу корисника (samparse, profilelist)

# Анализа артифаката оперативног система Windows

Скрипта алата RegRipper могу се груписати у неколико категорија:

– скрипта која приказују информације о инсталираним програмима (uninstall, apppaths, assoc, installedcomp, msis, product, installer, clsid, listsoft, fileexts, arpcache, startpage)

– скрипта која дају информације о мрежној конфигурацији (networkcards, nic, nic2, macaddr, shares, fw_config, routes, networklist, ssid, networkuid, network, termserv, termcert, rdpport, sql_lastconnect)

– скрипта која дају информације о екстерним складиштима (mountdev2, ide, usbdevices, usbstor, devclass, emdmgmt, wpdbusenum, bthport, btconfig, imagedev, stillimage, mp2, mndmru, knowdev, ddo)

# Анализа артифаката оперативног система Windows

Скрипта алата RegRipper могу се груписати у неколико категорија:

– скрипта која приказују информације о периферним уређајима (audiodev)

– скрипта која дају информације о извршеним програмима (prefetch, appcompatcache, legacy, tracing, at, direct, amcache, muicache, userassist, appcompatflags, winscp, mixer)

# Анализа артифаката оперативног система Windows

Скрипта алата RegRipper могу се груписати у неколико категорија:

– скрипта која дају информације о програмима чије извршавање започиње након покретања оперативног система (soft_run, user_run, services, svc, svcdll, appinitddls, init_dlls, bho, installedcomp, imagefile, winlogon, svchost, drivers32, cmd_shell, shellexec, shellext, schedagent, appcertdlls, lsa_packages, safeboot, dllsearch, securityproviders, load, winlogon_u, cmdproc, startup, cached, profiler, cmd_shell_u)

– скрипта која приказују информације о систему логовања системских и корисничких активности (mrt, auditpol, eventlog, eventlogs, winevt, auditfail, drwatson)

# Анализа артифаката оперативног система Windows

Скрипта алата RegRipper могу се груписати у неколико категорија:

– скрипта која указују на постојање малициозног програма (pending, netsvcs, inprocserver, fileless, cpldontload)

– скрипта која приказују информације о општим корисничким активностима (typedpaths, nmc, runmru, applets, acmru, wordwheelquery, cdstaginginfo, gthist)

– скрипта која приказују информације о мрежним активностима корисника (mndmru, compdecs, tsclient, rdphint, ssh_host_keys, winscp_sessions, vncviewer, vnchooksapplicationprefs)

# Анализа артифаката оперативног система Windows

Скрипта алата RegRipper могу се груписати у неколико категорија:

– скрипта која приказују информације о приступима датотекама од стране корисника (shellbags, itempos, comdlg32, recentdocs, winzip, winrar, sevenzip, mspaper, nero, officedocs, reading_locations, oisc, trustrecords, snaphost_viewer, adoberdr, wallpaper, mpmru, realplayer6)

– скрипта која дају информације о програмима за комуникацију (outlook, olsearch, unreadmail, skype, aim, liveContactsGUID, yahoo_cu)

# Анализа артифаката оперативног система Windows

Логови системске и корисничке активности (**Windows Event Logs**) су у формату **evtx** (Windows XML Event Log).

Да бисмо прочитали садржај ових логова, потребно га је парсирати.

За парсирање ових логова користићемо скрипта **evtx_dump.py**:

```
$ python2 /home/kali/.local/bin/evtx_dump.py
Application.evtx
```

Факултет техничких наука
Лабораторија за дигиталну форензику

# Linux
## (дистрибуција Ubuntu 14.04)


Светлана Антешевић, Милица Матијевић

# Прегледање и анализа артифаката оперативног система Linux

Увид у форензичку копију масовне меморије помоћу алата као што је Autopsy.

Увид у систем датотека масовне меморије помоћу форензичког моста, који спречава измену података на меморијском складишту.


Tableau форензички мост

# Прегледање и анализа артифаката оперативног система Linux

Директоријум који садржи системску конфигурацију: **`/etc/`** (садржи директоријуме и датотеке са конфигурационим параметрима система).

- ➔ `/etc/bash.bashrc` – команде које се изврше када се покрене *bash*
- ➔ `/etc/ca-certificates.conf` – листа ауторитативних тела за издавање Сертификата
- ➔ `/etc/fstab` – садржи локације маунтовања партиција
- ➔ `/etc/group` – листа корисничких група
- ➔ `/etc/hostname` – садржи име хоста
- ➔ `/etc/hosts` – садржи мапирање IP адресе и имена хоста
- ➔ `/etc/host.allow` – листа имена хостова којима је дозвољен приступ систему
- ➔ `/etc/host.deny` – листа имена хостова којима је забрањен приступ систему

# Прегледање и анализа артифаката оперативног система Linux

- ➔ `/etc/iftab` – листа мапирања комуникациони интерфејс–MAC адреса
- ➔ `/etc/login.defs` – списак локација лог датотека у вези са пријавом на систем
- ➔ `/etc/logrotate.conf` – специфицира период након кога се врши преписивање логова
- ➔ `/etc/lsb-release` – информације о оперативном систему
- ➔ `/etc/mailcap` – листа MIME типова и програма који парсирају садржај датих типова
- ➔ `/etc/mime.types` – листа MIME типова са екстензијама датотека чијем садржају одговарају
- ➔ `/etc/rsyslog.conf` – конфигурација система за управљање логовима – rsyslog
- ➔ `/etc/services` – листа мрежних сервиса са портовима
- ➔ `/etc/shadow` – складиште хешираних лозинки за пријаву на систем

# Прегледање и анализа артифаката оперативног система Linux

- ➔ `/etc/sysctl.conf` – поставке системских варијабли
- ➔ `/etc/timezone` – временска зона
- ➔ `/etc/dhcp/dhclient.conf` – конфигурација DHCP сервиса
- ➔ `/etc/pam.d/common-auth` – информације о криптографским механизмима који се користе за складиштење лозинки
- ➔ `/etc/rsyslog.d/50-default.conf` – иницијална конфигурација система за управљање логовима – rsyslog
- ➔ `/etc/sudoers` – садржи листу корисничких имена која имају администраторске привилегије

# Прегледање и анализа артифаката оперативног система Linux

Директоријум који садржи корисничку конфигурацију: **/home/** (садржи директоријуме и датотеке са конфигурационим параметрима корисника).

- ➔ `/home/<корисничко име>/.config/autostart` – садржи датотеке повезане са програмима који се покрећу након покретања оперативног система
- ➔ `/home/<корисничко име>/.local/share/recently-used.xbel` – информације о најскорије коришћеним датотекама
- ➔ `/home/<корисничко име>/.local/share/keyrings/user.keystore` – складиште криптографских кључева

# Прегледање и анализа артифаката оперативног система Linux

Директоријум који садржи системске и корисничке логове: **`/var/log/`**

- ➔ `/var/log/kern.log` – информације о прикључиваним USB уређајима, комуникационим интерфејсима и времену у току кога је рачунар био у стању *suspended*
- ➔ `/var/log/dpkg.log` – информације о времену инсталације, деинсталације и ажурирања програма
- ➔ `/var/log/wtmp` – историја успешних пријава корисника на систем и одјава са система
- ➔ `/var/log/btmp` – историја неуспешних пријава корисника на систем

# Процес форензичке истраге


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

# Анализа артифаката оперативног система Linux

- ➔ Конфигурационе датотеке и логови активности су у текстуалном формату (читљиви човеку).
- ➔ Изузетак представљају логови корисничких пријава на систем – **wtmp** и **btmp**.
- ➔ Алат способан за парсирање датотека wtmp и btmp је **utmpdump**.

  $ **utmpdump** wtmp

- ➔ У оквиру алата Autopsy могуће је прочитати садржај текстуалних датотека.
- ➔ Уколико алат Autopsy не пружа потпун увид у садржај датотеке, потребно ју је извести и анализирати у неком од текстуалних едитора.

# Процес форензичке истраге


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

# Презентација

Резултати анализе доказа се презентују у писменом облику.

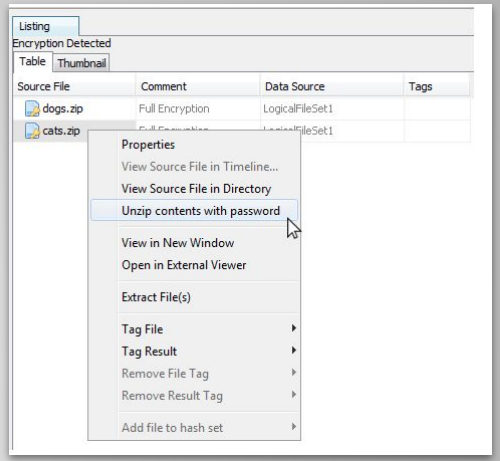
Односи се на процес којим форензичар дели резултате фазе анализе у облику извештаја заинтересованим странама.

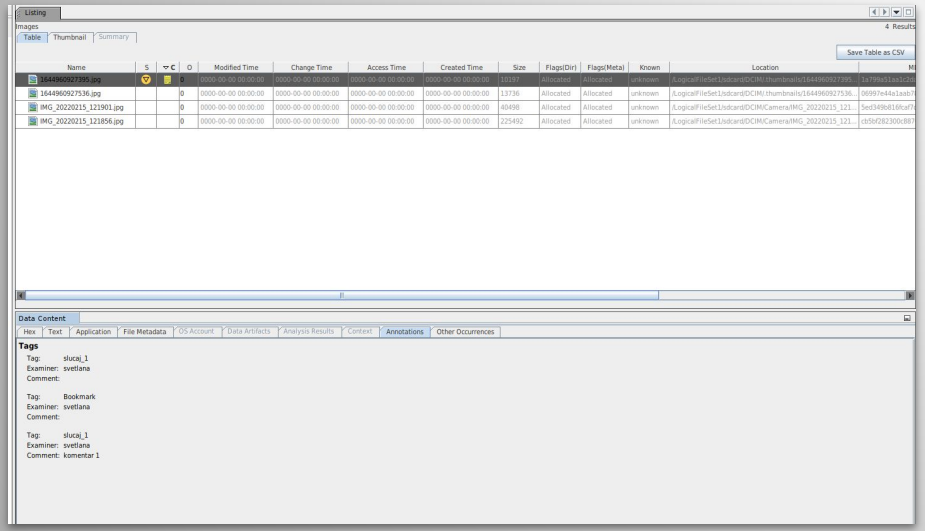
Форензичар обично сачињава налаз и мишљење и усмено га брани одговарајући на питања на главном судском претресу.

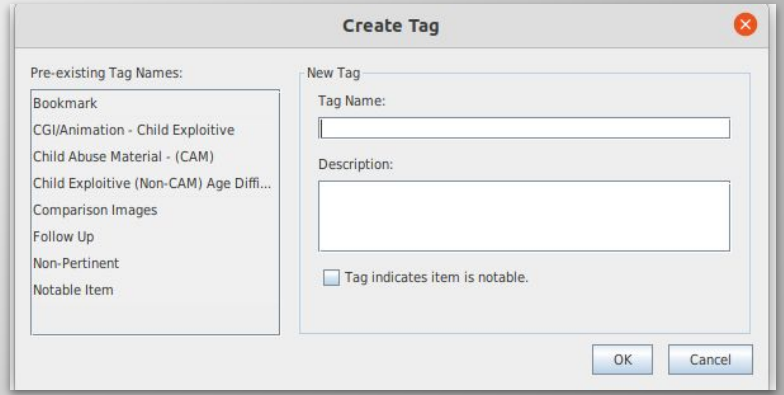
# Презентација

## Autopsy & The Sleuth Kit

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



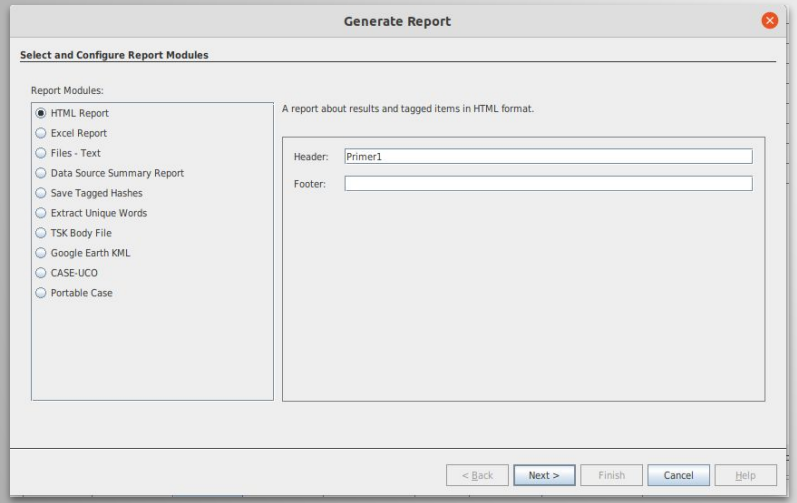



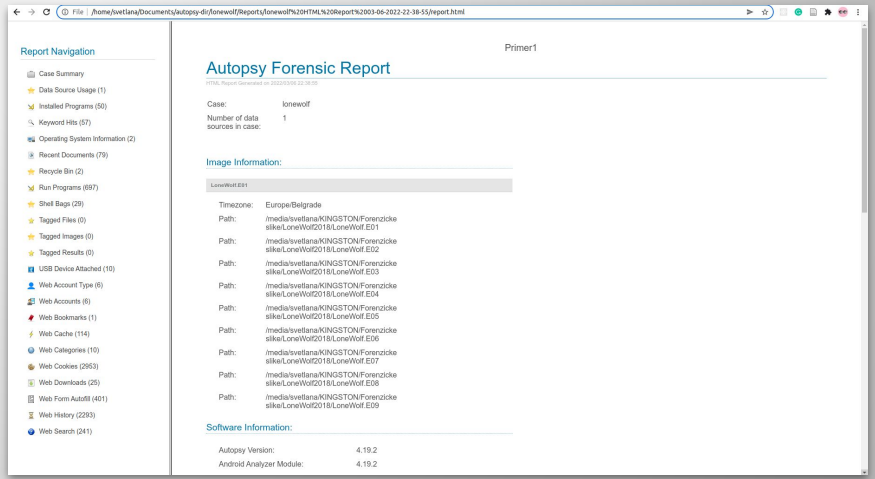



# Презентација

## Autopsy & The Sleuth Kit

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



# Коришћени алати

– Autopsy, https://www.autopsy.com/

– RegRipper3.0, https://github.com/keydet89/RegRipper3.0

– evtx_dump.py, https://pypi.org/project/python-evtx/