



Факултет техничких наука
Лабораторија за дигиталну форензику

ДИГИТАЛНА АНТИФОРЕНЗИКА

Увод у дигиталну форензику
Јелена Драгишић, Светлана Антешевић

Преглед области

Чиме се бави дигитална антифорензика?

Дигитална антифорензика је процес компромитовања доступности, поузданости и корисности дигиталних доказа током процеса дигиталне форензичке истраге.

Преглед области

Где се све примењује антифорензика?

- Технике дигиталне антифорензике могу да се користе у сврху очувања података на уређајима, обезбеђивању података и смањивању ризика.
- Док са друге стране могу да се користе у сврху уништавања доказа, крађе и злоупотребе података.

Преглед области

Који су то индикатори дигиталне антифорензике?

- Шифровани подаци (пре су били индикатори, данас је све шифровано)
- Докази о брисању артефаката
- Докази о скривању трагова
- Присуство антифорензичких алата
- Присуство форензичких алата



Факултет техничких наука
Лабораторија за дигиталну форензику

АНТИФОРЕНЗИЧКЕ ТЕХНИКЕ

Антифорензичке технике



**СКРИВАЊЕ
ПОДАТКА**

● ШИФРОВАЊЕ

● СТЕГАНОГРАФИЈА

● КОНТРАЦЕПЦИЈА ПОДАТКА

● МАНИПУЛАЦИЈА СИСТЕМОМ ДАТОТЕКА

● МАНИПУЛАЦИЈА ЧВРСТИМ ДИСКОМ

● СКРИВАЊЕ У МЕМОРИЈИ

● СКРИВАЊЕ У МРЕЖИ

Стеганографија

Пример 1. Скривање текста унутар фотографије

StegHide - алат који може да сакрије податке у различитим врстама датотека (jpeg, bmp, wav). Може да врши компресију, шифровање, екстраховање података.

```
$ steghide embed -cf novi_sad.jpg -ef skrivena_poruka.txt
```

Enter passphrase:

```
$ steghide extract -sf novi_sad.jpg
```

Enter passphrase:

StegSeek - алат који може да крекује датотеке над којима је примењена стеганографија помоћу StegHide алата и изврши стеганализу.

```
$ stegseek --crack novi_sad.jpg rockyou.txt <output.txt>
```


**СКРИВАЊЕ
ПОДАТКА**

● ШИФРОВАЊЕ

● СТЕГАНОГРАФИЈА

● КОНТРАЦЕПЦИЈА ПОДАТКА

● МАНИПУЛАЦИЈА СИСТЕМОМ ДАТОТЕКА

● МАНИПУЛАЦИЈА ЧВРСТИМ ДИСКОМ

● СКРИВАЊЕ У МЕМОРИЈИ

● СКРИВАЊЕ У МРЕЖИ

Контрацепција података

SYSCALL PROXYING

Syscall proxying преставља процес пресретања системских позива које програм шаље језгру оперативног система (I/O операције над датотекама, мрежну комуникацију, управљање процесима..) и врши преусмеравање ка proxy серверу.

На тај начин се врши посредно позивање системских функција помоћу proxy-а тј. симулира се удаљено извршавање програма.

Syscall (system calls) представља најнижи ниво комуникације између кернела и корисничког режима.

Пример: Нападач жели да изврши злонамерну активност, као што је пресретање системског позива за слање података путем мреже и модификација тих података пре него што буду послати.

Контрацепција података

SYSCALL PROXYING

Детектовање коришћења:

- Праћење системских позива који се извршавају на рачунару.
- Провера интегритета система коришћењем програма за детекцију промена у фајловима или проверу хеш вредности.
- Анализом мрежног саобраћаја могу се детектовати сумњиве активности, неуобичајене адресе, портови.
- Праћењем перформанси рачунара могу се детектовати падови перформанси, успорен рад система, високо оптерећење CPU-а или мреже без очигледног разлога.
- Коришћење антивирусних и сигурносних алата који могу детектовати злонамерни софтвер или активност на рачунару.

Контрацепција података

REMOTE LIBRARY INJECTION

Remote Library Injection - односи се на сигурносну рањивост и технику напада која укључује уметање злонамерног кода у динамички повезане библиотеке удаљеног система. Представља једну од метода која може да компромитује неки рачунар. Може се користити у комбинацији са syscall proxying.

DLL (Dynamic Link Library - Windows) и .so (Shared Library - Linux) датотеке су датотеке заједничке библиотеке које омогућавају да код (а понекад и податке) деле различити процеси.

Пример: Нападач искориштава рањивост у веб апликацији и удаљено мења библиотеку коју апликација користи. Када се измењена библиотека користи, злонамерни код нападача се извршава, омогућавајући му чување података или преузимање контроле над сервером.

Контрацепција података

REMOTE LIBRARY INJECTIONS

Нуспојаве:

- Ограничавање приступа API позивима.
- Спречавање исправног рада легитимног софтвера.
- Ублажавање идентификовања или блокирања злонамерног софтвера.
- Подизање привилегија злонамерном софтверу.
- Може да зарази ваш рачунар са одређеним вирусима.

Детектовање коришћења:

- Скенирање система за рањивост и неправилност.
- Праћење и анализа логова за сумњиве активности.
- Мониторинг мрежног саобраћаја у потрази за неправилностима.
- Коришћење специјализованих сигурносних алата или IDS/IPS система.
- Редовно ажурирање софтвера и библиотека.

Контрацепција података

DIRECT KERNEL OBJECT MANIPULATION - DKOM

DKOM (Direct Kernel Object Manipulation) је техника која омогућава директну манипулацију објектима у језгру оперативног система, као што су Windows и Linux. Користи се у развоју, анализи и сигурносном тестирању софтвера на ниском нивоу.

DKOM је уобичајена техника rootkit-а за скривање потенцијално штетних процеса, драјвера, датотека и посредних веза трећих страна од *task manager* и *event scheduler*.

Rootkits и антивирусни програми делују као део ос тако да имају приступ меморији кернела и могу се сакрити од системске табеле и *task manager*-а.

Могуће је детектовати присуство rootkit-а проверавањем употребе CPU, текућег и одлазног мрежног саобраћаја, покренутих процеса или потписа драјвера.

Контрацепција података

ПРЕНОСНЕ АПЛИКАЦИЈЕ

Могуће је неке апликације инсталирати на неком преносном медијуму за складиштење (нпр. USB) и покренути их на њима.

Пример: Коришћење преносивог веб претраживача како би се скрили докази о почињавању неких кривичних дела путем интернета.

Веб претраживачи имају могућност покретања приватног режима апликације.

Помоћу форензике радне меморије могу се открити одређени докази о коришћењу интернета.

Више о томе у раду на следећем [линку](#).

Контрацепција података

Пример 2. Скривање процеса на Linux-у

Користићемо пример са следећег [линка](#).

- **evil_script.py** - представља python скрипту која може да обави неку злонамерну активност као што је слање UDP пакета трећој особи.
- **processhider.c** - представља C библиотеку која је у стању да модификује libc (C стандардна библиотека која поседује функције као што су *opendir()* и *readdir()*). Базирана је на функцији *Linux dinamic linker*-а који служи као компонента која брине о учитавању различитих библиотека које су потребне програму током времена извршавања, што је везано за *preloading* функцију. Са *preloading*-ом имамо могућност да учитамо нашу библиотеку пре него што се читају неке друге системске библиотеке. И да у нашој библиотеци имплементирамо замену за *readdir()* функцију *libc* библиотеке и да том логиком сакријемо процес.
- Логика : сваки пут када се чита */proc/PID* директоријум (где је PID pid процеса који има име „evil_script“) блокирамо тај приступ.

Контрацепција података

Пример 2. Скривање процеса на Linux-у

Покретање **evil_script.py**

```
$ cd libprocesshider/  
$ ./evil_script.py
```

Листа свих покренутих процеса који у називу имају реч “evil”

```
$ ps aux | grep -i evil
```

Компајлирање **processhider.c** библиотеке

```
$ make
```

Учитати библиотеку помоћу global dynamic linker-a [root привилегија - \$ **sudo su**]

```
# sudo mv libprocesshider.so /usr/local/lib/  
# echo /usr/local/lib/libprocesshider.so >> /etc/ld.so.preload
```

Контрацепција података

Пример 2. Скривање процеса на Linux-у

Sysdig - алат који може да детектује скривене процесе на рачунару

```
# sudo sysdig -c topprocs_cpu  
# sudo sysdig proc.name contains evil
```

**СКРИВАЊЕ
ПОДАТКА**

● ШИФРОВАЊЕ

● СТЕГАНОГРАФИЈА

● КОНТРАЦЕПЦИЈА ПОДАТКА

● МАНИПУЛАЦИЈА СИСТЕМОМ ДАТОТЕКА

● МАНИПУЛАЦИЈА ЧВРСТИМ ДИСКОМ

● СКРИВАЊЕ У МЕМОРИЈИ

● СКРИВАЊЕ У МРЕЖИ

Манипулација системом датотека

СКРИВАЊЕ ДИРЕКТОРИЈУМА ИЛИ ДАТОТЕКЕ

Пример 3. Скривање датотека/директоријума или датотеке на Linux-y

```
$ mv datoteka.txt .skrivena_datoteka.txt  
$ mv direktorijum/ .skriveni_direktorijum/
```

Преглед скривених датотека/директоријума

```
$ ls -a  
$ ls -al
```


Манипулација системом датотека

ИЗМЕНА МЕТАПОДАТКА

Пример 4. Измена метаподатака помоћу Exiftool алата

```
$ exiftool -Artist='Ime Prezime' -overwrite_original promena_metapodataka.jpg  
$ exiftool -Copyright='Ime Prezime' -overwrite_original promena_metapodataka.jpg
```

Пример 5. Промена временских ознака на рачунару - *Changing timestamps*

```
$ sudo su  
# dpkg-reconfigure tzdata
```

```
(root@kali)-[~]  
# dpkg-reconfigure tzdata  
  
Current default time zone: 'Europe/Belgrade'  
Local time is now:      Mon May 30 22:40:48 CEST 2022.  
Universal Time is now:  Mon May 30 20:40:48 UTC 2022.
```

Манипулација системом датотека

АЛТЕРНАТИВНИ ТОКОВИ ПОДАТКА

Пример 6. Промена екстензије датотеке

```
$ mv slika.jpg slika.txt
```

Autopsy Ingest Modul - File Type Mismatch - може да детектује измењену екстензију датотеке.

Alternate Data Streams на Windows-у омогућава скривање једне датотеке унутар друге датотеке. Блог о томе на [линку](#).

**СКРИВАЊЕ
ПОДАТКА**

● ШИФРОВАЊЕ

● СТЕГАНОГРАФИЈА

● КОНТРАЦЕПЦИЈА ПОДАТКА

● МАНИПУЛАЦИЈА СИСТЕМОМ ДАТОТЕКА

● МАНИПУЛАЦИЈА ЧВРСТИМ ДИСКОМ

● СКРИВАЊЕ У МЕМОРИЈИ

● СКРИВАЊЕ У МРЕЖИ

Манипулација чврстим диском

СКРИВАЊЕ ПАРТИЦИЈА

Пример 7. Скривање партиција на Linux-у

Gparted - алат који даје преглед партиција на Linux оперативним системима.

Команда која даје преглед партиција на диску кроз терминал.

```
$ sudo fdisk -l
```

Унутар директоријума `/etc/udev/rules.d/` могуће је креирати нека системска правила. Датотеке које се креирају унутар овог директоријума се конвенционално називају бројем као префиксом и обрађују се у лексичком редоследу независно од директоријума у којем се налазе.

```
$ sudo touch /etc/udev/rules.d/99-hide-partitions.rules
$ sudo su
# nano /etc/udev/rules.d/99-hide-partitions.rules
KERNEL=="sdb", ENV{UDISKS_IGNORE}="1"
# cat /etc/udev/rules.d/99-hide-partitions.rules
# udevadm control --reload-rules && udevadm trigger -> Umesto # reboot
```

Манипулација чврстим диском

СКРИВАЊЕ УНУТАР SLACK SPACE-A

Slack space - део последњег блока придруженог датотеци који не складишти податке текуће датотеке. У њему могу да се нађу подаци о некој датотеци којој је раније био придружен тај блок. Постоје алати који могу да поврате податке из slack space-a.

Могуће је уписати неке податке/сакрити унутар slack space-a.

Блок је основна јединица за читање и писање података на хардверском нивоу. Уобичајено је величина блока 512 бајтова (4096 битова).

ОС пишу податке у кластере/секторе који се састоје од блокова.

Манипулација чврстим диском

СКРИВАЊЕ УНУТАР SLACK SPACE-A

Пример 8. Скривање поруке унутар slack space-а датотеке на диску

Унутар slack_space директоријума постоји slack_space_datoteka.txt која ће нам послужити за пример, slack_space_komande.txt датотека у оквиру које су остављене команде које је потребно извршити и slack_space.py python скрипта која врши скривање унутар блока датотеке.

```
$ cd /slack_space
$ sudo fdisk -l -> Увид у све дискове и партиције
$ sudo lsblk -> Увид у све mount-оване локације које су блок оријентисане
$ sudo tune2fs -l /dev/sdb | grep -i 'block size' -> Величина блока за
писање на диску
# потребно је сместити датотеку на одговарајући диск и изделити је на више
мањих
# одабрати датотеку чији је капацитет мањи од једног блока за писање(нпр.
хаа) и израчунати њену хеш вредност пре скривања поруке
$ stat хаа -> Враћа Inode прослеђене датотеке, режим приступа, власништво,
датум креирања, тип датотеке..
```


Манипулација чврстим диском

СКРИВАЊЕ УНУТАР SLACK SPACE-A

Пример 8. Скривање поруке унутар slack space-а датотеке на диску

```
$ sudo debugfs -R "stat <13>" /dev/sdb -> Враћа број EXTENDS, где код -R
наводимо Inode број датотеке и путању до логичке партиције диска. EXTENDS -
непрекидна област складиштења резервисана за датотеку у систему датотека
# потребно изменити slack_space.py скрипту по упутствима у њој и покренути
помоћу команде
# скрипта смешта скривену поруку унутар блока и чита податке из одређеног
блока, па је помоћу ње могуће и увидети скривену поруку.
$ sudo python3.9 slack_space.py > rezultat.txt
# проверити хеш вредност датотеке у оквиру чијег блока смо сместили поруку.
```

Манипулација чврстим диском

СКРИВАЊЕ УНУТАР ПОКВАРЕНИХ БЛОКОВА

Покварен блок (bad block) је део медија за складиштење који више није поуздан за складиштење и преузимање података јер је физички оштећен или покварен усред неких радњи на рачунару.

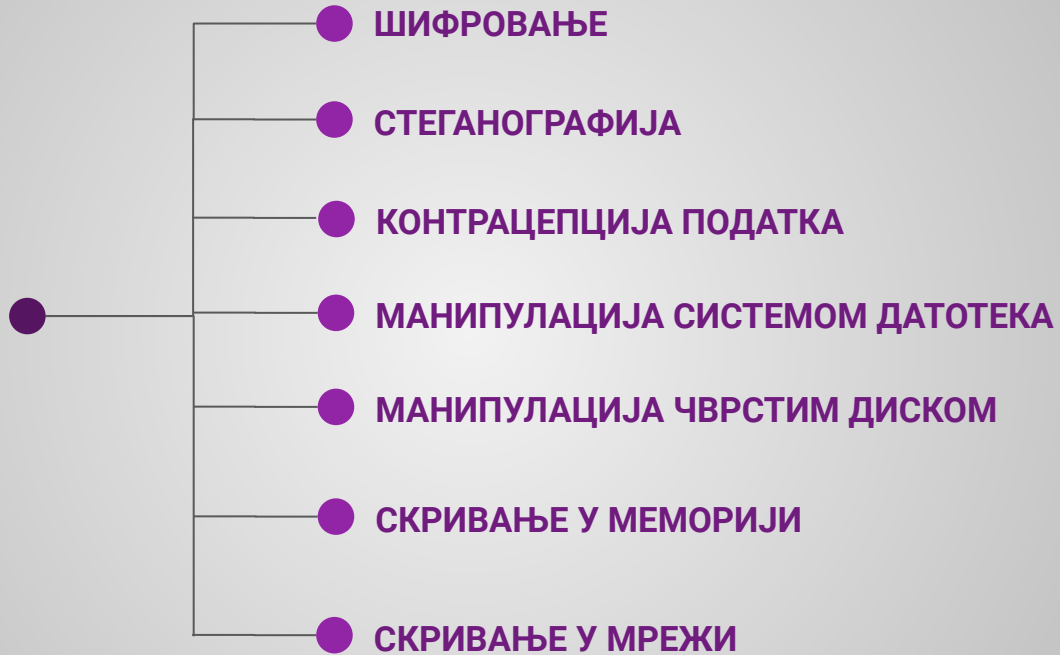
Такође могуће је и да у табели на нивоу фајл система означимо исправне блокове као покварене, а да у њима сместимо неке податке које желимо да сакријемо.

Постоје алати који могу да детектују покварене блокове, један од њих је **badblocks** - алат командне линкије који претражује покварене блокове унутар одређених партиција.

```
$ sudo badblocks -s /dev/sdb1
```

-s - Даје процентуални приказ прегледаних блокова.

**СКРИВАЊЕ
ПОДАТКА**



Антифорензичке технике



БРИСАЊЕ АРТЕФАКАТА

- ТЕХНИКЕ РАЗМАГНЕТИСАЊА ИЛИ УНИШТАВАЊА ДИСКОВА
- БРИСАЊЕ ДИСКОВА
- БРИСАЊЕ ДАТОТЕКА
- БРИСАЊЕ МЕТАПОДАТАКА
- БРИСАЊЕ РЕГИСТАРА
- БРИСАЊЕ ЛОГ ДАТОТЕКА
- БРИСАЊЕ СПОЉАШЊИХ МЕДИЈУМА
- ГЕНЕРИЧКО БРИСАЊЕ ПОДАТКА

Брисање дискова

Преписивање податка на партицији и брисање

Shred - алат који може да изврши преписивање податка на Linux-y

```
$ fdisk -l  
$ sudo shred -vzf /dev/sde
```

Shred алат има доста опција:

- n - број преписа. Подразумевано је три.
- u - преписати и избрисати.
- s - број бајтова за уситњавање.
- v - прикажи проширене информације.
- f - принудна промену дозвола да би се омогућило писање ако је потребно.
- z - додајте коначно преписивање са нулама да бисте сакрили коришћење алата.

БРИСАЊЕ АРТЕФАКАТА

- ТЕХНИКЕ РАЗМАГНЕТИСАЊА ИЛИ УНИШТАВАЊА ДИСКОВА
- БРИСАЊЕ ДИСКОВА
- БРИСАЊЕ ДАТОТЕКА
- БРИСАЊЕ МЕТАПОДАТАКА
- БРИСАЊЕ РЕГИСТАРА
- БРИСАЊЕ ЛОГ ДАТОТЕКА
- БРИСАЊЕ СПОЉАШЊИХ МЕДИЈУМА
- ГЕНЕРИЧКО БРИСАЊЕ ПОДАТКА

Брисање датотека

Пример 9. Преписивање податка у датотеци и брисање

Shred - алат који може да изврши преписивање податка на Linux-у

```
$ sudo shred -vzu -n5 nesto.txt
```

Постоје алати за опоравак избрисаних датотека/партиција: [Foremost](#), [Scalpel](#), [Testdisk](#)

БРИСАЊЕ АРТЕФАКАТА

- ТЕХНИКЕ РАЗМАГНЕТИСАЊА ИЛИ УНИШТАВАЊА ДИСКОВА
- БРИСАЊЕ ДИСКОВА
- БРИСАЊЕ ДАТОТЕКА
- БРИСАЊЕ МЕТАПОДАТАКА
- БРИСАЊЕ РЕГИСТАРА
- БРИСАЊЕ ЛОГ ДАТОТЕКА
- БРИСАЊЕ СПОЉАШЊИХ МЕДИЈУМА
- ГЕНЕРИЧКО БРИСАЊЕ ПОДАТКА

Брисање метаподатака

Пример 10. Брисање метаподатка фотографије

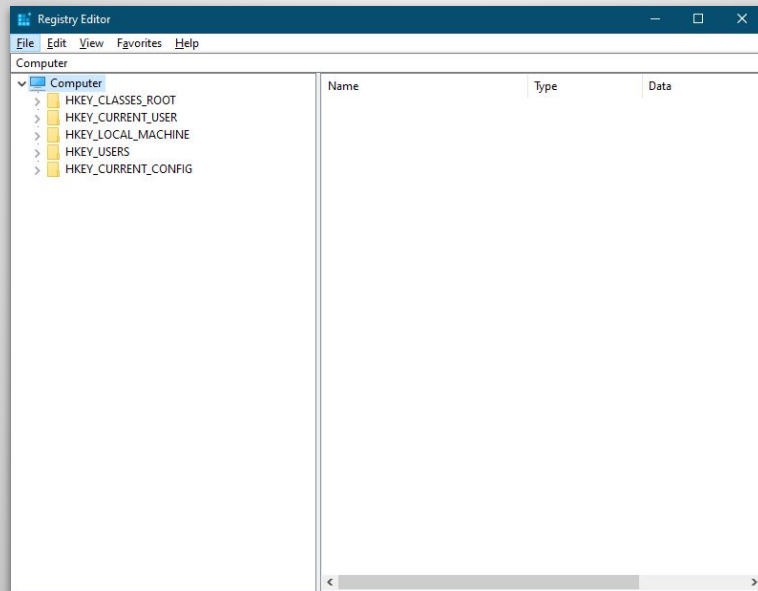
```
$ exiftool -all= -overwrite_original slika.jpg
```

БРИСАЊЕ АРТЕФАКАТА

- ТЕХНИКЕ РАЗМАГНЕТИСАЊА ИЛИ УНИШТАВАЊА ДИСКОВА
- БРИСАЊЕ ДИСКОВА
- БРИСАЊЕ ДАТОТЕКА
- БРИСАЊЕ МЕТАПОДАТАКА
- БРИСАЊЕ РЕГИСТАРА
- БРИСАЊЕ ЛОГ ДАТОТЕКА
- БРИСАЊЕ СПОЉАШЊИХ МЕДИЈУМА
- ГЕНЕРИЧКО БРИСАЊЕ ПОДАТКА

Брисање регистара

Пример: Брисање конфигурационих датотека на Windows помоћу *RegistryEditor*-а. Овом опцијом нећемо моћи да обављамо уобичајене активности на рачунару. Ништа неће бити дозвољено. Чак нећемо моћи ни да угасимо рачачунар одабиром опције ShutDown.



БРИСАЊЕ АРТЕФАКАТА

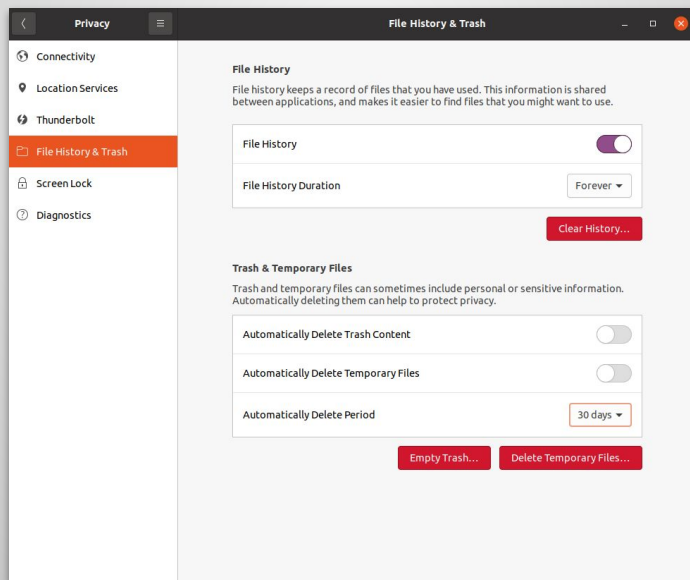
- ТЕХНИКЕ РАЗМАГНЕТИСАЊА ИЛИ УНИШТАВАЊА ДИСКОВА
- БРИСАЊЕ ДИСКОВА
- БРИСАЊЕ ДАТОТЕКА
- БРИСАЊЕ МЕТАПОДАТАКА
- БРИСАЊЕ РЕГИСТАРА
- БРИСАЊЕ ЛОГ ДАТОТЕКА
- БРИСАЊЕ СПОЉАШЊИХ МЕДИЈУМА
- ГЕНЕРИЧКО БРИСАЊЕ ПОДАТКА

Брисање лог датотека

Брисање лог датотека на linux-y

```
# ls -l /var/log/messages  
# rm /var/log/message
```

Могуће је обрисати историју коју чува Linux кроз **Settings/Privacy/File History and Trash**.



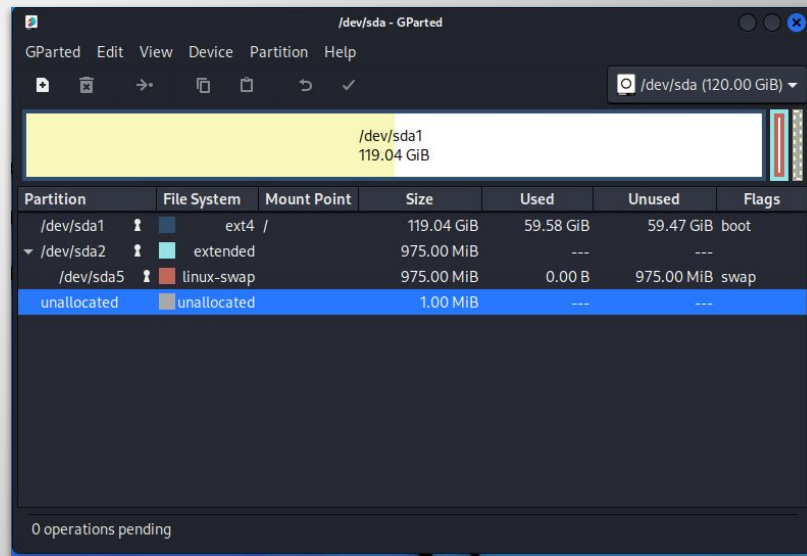
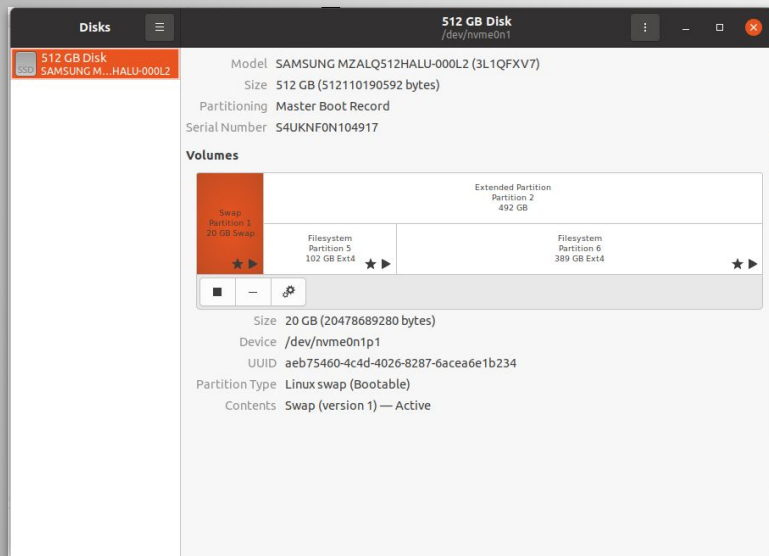
БРИСАЊЕ АРТЕФАКАТА

- ТЕХНИКЕ РАЗМАГНЕТИСАЊА ИЛИ УНИШТАВАЊА ДИСКОВА
- БРИСАЊЕ ДИСКОВА
- БРИСАЊЕ ДАТОТЕКА
- БРИСАЊЕ МЕТАПОДАТАКА
- БРИСАЊЕ РЕГИСТАРА
- БРИСАЊЕ ЛОГ ДАТОТЕКА
- БРИСАЊЕ СПОЉАШЊИХ МЕДИЈУМА
- ГЕНЕРИЧКО БРИСАЊЕ ПОДАТКА

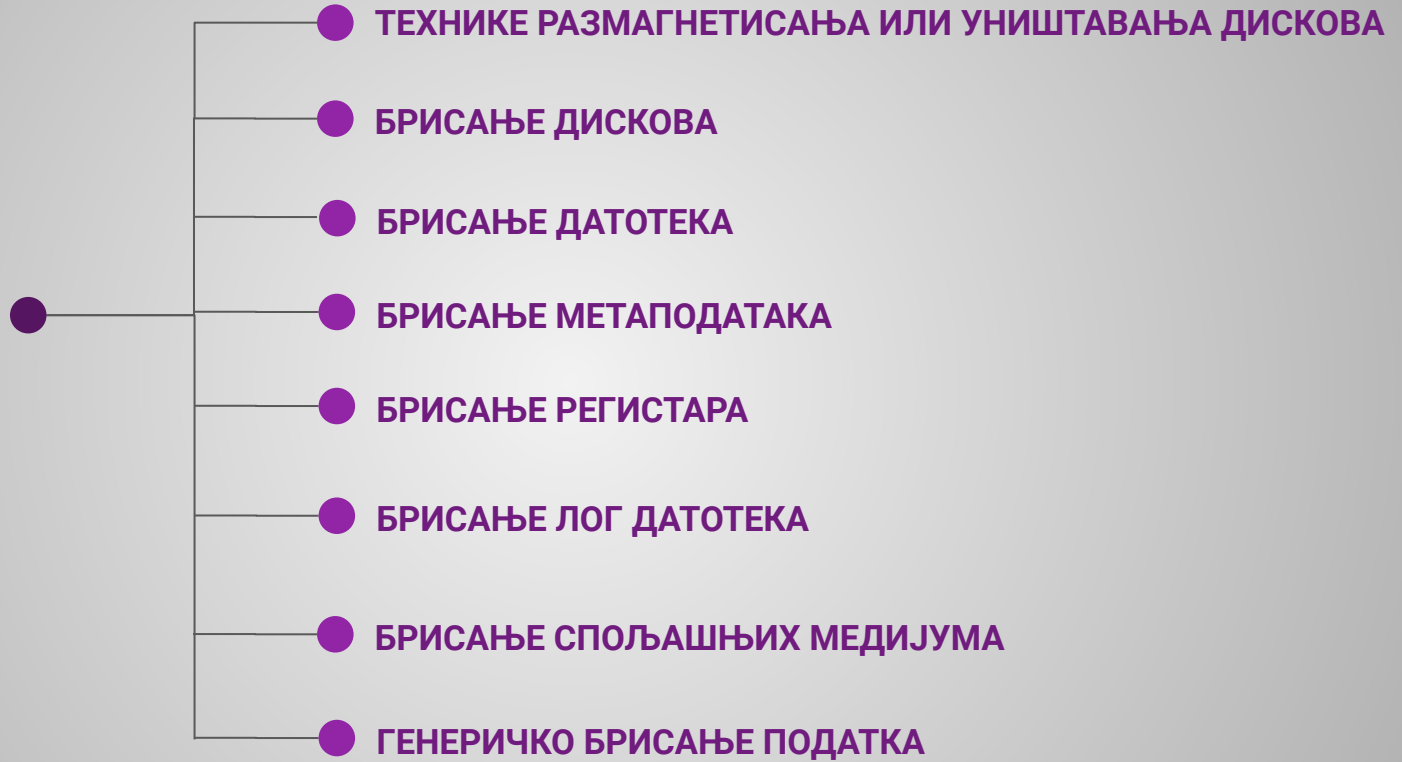
Брисање спољашњих медијума

Брисање података на USB диску

- **Disks** - алат на Linux-у који служи за форматирање, брисање и моунтовање дискова.
- **Gparted** - алат на Kali Linux-у.



БРИСАЊЕ АРТЕФАКАТА



Антифорензичке технике



СКРИВАЊЕ ТРАГОВА

- ЛАЖИРАЊЕ IP АДРЕСЕ
- ЛАЖИРАЊЕ MAC АДРЕСЕ
- МАНИПУЛАЦИЈА ЛОГ ДАТОТЕКАМА
- КОРИШЋЕЊЕ PROXY СЕРВЕРА И VPN-a
- КОРИШЋЕЊЕ THE ONION ROUTER (TOR) ПРОТОКОЛА
- КОРИШЋЕЊЕ ЗОМБИ НАЛОГА

Лажирање IP адресе

IP адреса се појављује на OSI 3 нивоу - IP протокол.

Могуће је изменити тј. лажирати IP адресу на неком рачунару унутар неке мреже, али ако је та мрежа добро конфигурисана не би смела да дозволи ту могућност и аутоматски ће нас искључити из мреже.

Ifconfig - алат који даје увид у IP, MAC адресу, мрежну маску на рачунару.

```
$ ifconfig  
$ sudo ifconfig eth0 10.0.2.10 netmask 255.255.255.0  
$ ifconfig
```

Лажирање IP адресе

```
(test@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.69 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe0e:348d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0e:34:8d txqueuelen 1000 (Ethernet)
    RX packets 41 bytes 36938 (36.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 41 bytes 3358 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(test@kali)-[~]
└─$ sudo ifconfig eth0 10.0.2.10 netmask 255.255.255.0
[sudo] password for test:

(test@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.10 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe0e:348d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0e:34:8d txqueuelen 1000 (Ethernet)
    RX packets 41 bytes 36938 (36.0 KiB)
```

СКРИВАЊЕ ТРАГОВА

- ЛАЖИРАЊЕ IP АДРЕСЕ
- ЛАЖИРАЊЕ MAC АДРЕСЕ
- МАНИПУЛАЦИЈА ЛОГ ДАТОТЕКАМА
- КОРИШЋЕЊЕ PROXY СЕРВЕРА И VPN-a
- КОРИШЋЕЊЕ THE ONION ROUTER (TOR) ПРОТОКОЛА
- КОРИШЋЕЊЕ ЗОМБИ НАЛОГА

Лажирање MAC адресе

Пример 11. Измена MAC адресе на рачунару

Macchanger - алат који служи за измену MAC адресе на linux-y

```
$ ifconfig
$ sudo macchanger -s eth0 -> провера тас адресе
$ sudo ifconfig eth0 down -> заустављање рада eth0 интерфејса
$ sudo macchanger -r eth0 -> измена тас адресе неком рандом адресом
$ sudo ifconfig eth0 up -> подизање eth0 интерфејса
$ sudo macchanger -s eth0 -> провера тас адресе
```

```
$ sudo macchanger -s eth0
$ sudo ifconfig eth0 down
$ sudo macchanger --mac 08:00:24:69:4c:47 eth0 -> измена тас адресе неком
дефинисаном адресом
$ sudo ifconfig eth0 up
$ sudo macchanger -s eth0
```

**СКРИВАЊЕ
ТРАГОВА**

- **ЛАЖИРАЊЕ IP АДРЕСЕ**
- **ЛАЖИРАЊЕ MAC АДРЕСЕ**
- **МАНИПУЛАЦИЈА ЛОГ ДАТОТЕКАМА**
- **КОРИШЋЕЊЕ PROXY СЕРВЕРА И VPN-a**
- **КОРИШЋЕЊЕ THE ONION ROUTER (TOR) ПРОТОКОЛА**
- **КОРИШЋЕЊЕ ЗОМБИ НАЛОГА**

Манипулација лог датотекама

Односи се на измену лог датотека на мрежним уређајима.

Пример: Уколико имамо приступ рутеру који је конфигуриран да обавља улогу DHCP сервера тј. да врши додељивање IP адреса. Можемо приступити његовој лог датотеци и изменити податке, нпр. своју IP адресу.

**СКРИВАЊЕ
ТРАГОВА**

- **ЛАЖИРАЊЕ IP АДРЕСЕ**
- **ЛАЖИРАЊЕ MAC АДРЕСЕ**
- **МАНИПУЛАЦИЈА ЛОГ ДАТОТЕКАМА**
- **КОРИШЋЕЊЕ PROXY СЕРВЕРА И VPN-а**
- **КОРИШЋЕЊЕ THE ONION ROUTER (TOR) ПРОТОКОЛА**
- **КОРИШЋЕЊЕ ЗОМБИ НАЛОГА**

Коришћење проху сервера

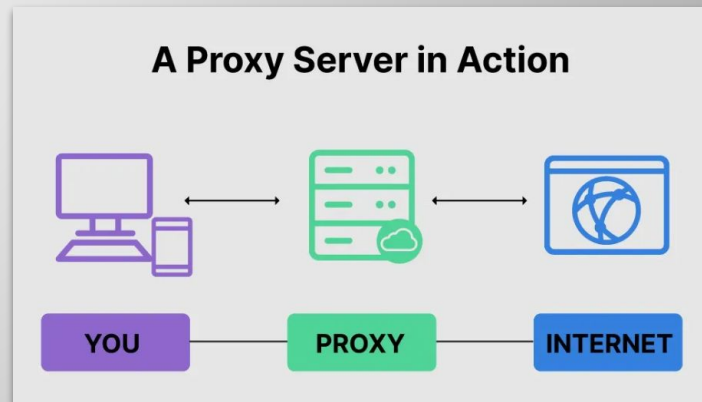
Proxy сервер је серверска апликација која делује као посредник између клијента који захтева ресурс и сервера који тај ресурс обезбеђује.

Обезбеђује нам анонимност тиме што удаљени сервер не зна ко му је стварно приступио, пошто види адресу проху сервера.

Односи се на апликативни ниво и не врши енкрипцију саобраћаја.

Функционалности Proxy сервера:

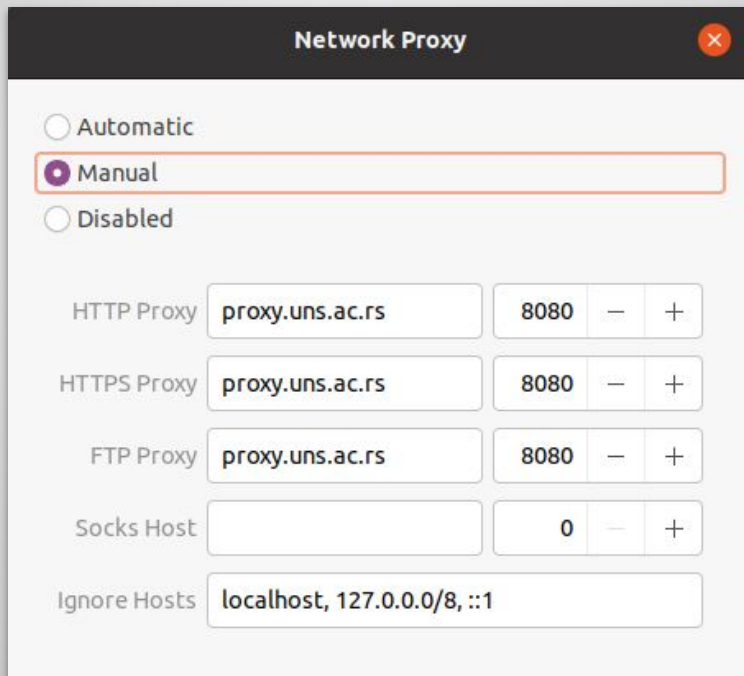
- Може да прати притуп на интернету
- Може да онемогући приступање одређеним интернет страницама
- Може да кешира интернет странице у бази податка и да омогући бржу комуникацију



Коришћење проху сервера

Подешавање проху сервера на linux-y

У оквиру **Settings/Network/Network Proxy** можемо да подесимо прокси.



Network Proxy

☐ Automatic

☒ Manual

☐ Disabled

HTTP Proxy proxy.uns.ac.rs 8080 − +

HTTPS Proxy proxy.uns.ac.rs 8080 − +

FTP Proxy proxy.uns.ac.rs 8080 − +

Socks Host 0 − +

Ignore Hosts localhost, 127.0.0.0/8, ::1

Коришћење VPN-а

VPN (Virtual Private Network) проширује приватну мрежу преко јавне мреже и омогућава корисницима да шаљу и примају податке преко заједничких или јавних мрежа као да су њихови рачунарски уређаји директно повезани на приватну мрежу. Односи се на ниво оперативног система. Углавном се плаћа.

Употребном VPN-а врши се енкрипција саобраћаја на мрежи и комуникација је успорена.

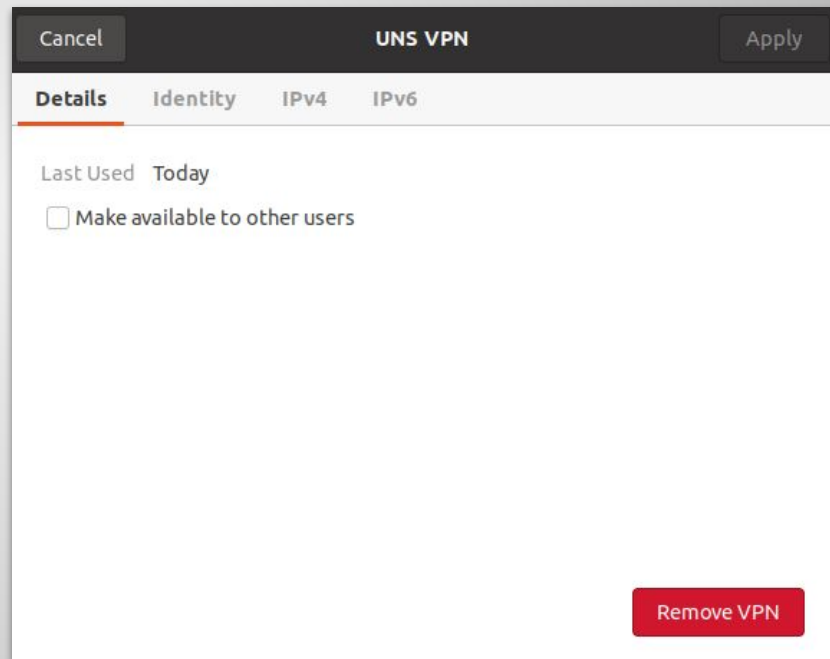
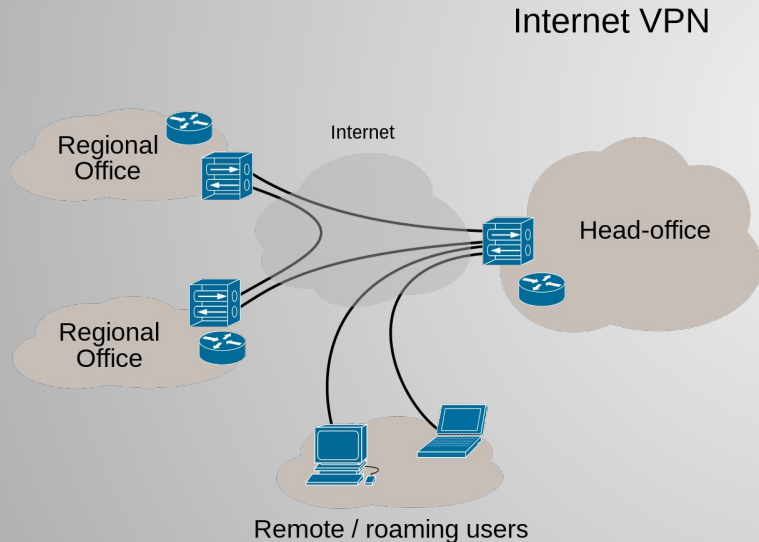
VPN мрежа може да буде праћена од стране треће стране (полиције, владиних организација..)

Могуће је употребом VPN-а приступити мрежи која се налази на другој локацији и биће нам додељена IP адреса из те мреже, тако да нам се не види наша и можемо да обавимо неку злонамерну активност.

Коришћење VPN-а

Подешавање VPN-а на linux-у

У оквиру **Settings/Network/VPN** можемо да подесимо конфигурацију VPN-а.



**СКРИВАЊЕ
ТРАГОВА**

- **ЛАЖИРАЊЕ IP АДРЕСЕ**
- **ЛАЖИРАЊЕ MAC АДРЕСЕ**
- **МАНИПУЛАЦИЈА ЛОГ ДАТОТЕКАМА**
- **КОРИШЋЕЊЕ PROXY СЕРВЕРА И VPN-a**
- **КОРИШЋЕЊЕ THE ONION ROUTER (TOR) ПРОТОКОЛА**
- **КОРИШЋЕЊЕ ЗОМБИ НАЛОГА**

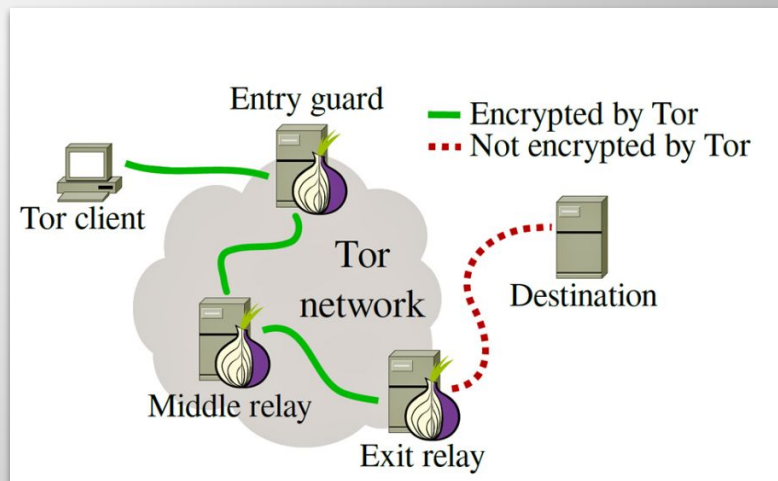
Коришћење TOR протокола



The Onion Routing је техника која се користи за анонимну комуникацију преко мреже где су поруке шифроване на слојевит начин.

Омогућава сакривање IP адресе, интернет активности и употребу мреже. Подаци пролазе кроз више мрежних чворова, сваки са слојевитом енкрипцијом.

Мана је што има одређено кашњење пакета, па неки streaming или слање видео снимака може да потраје. Такође одређене странице могу да блокирају приступ употребом TOR browsera.



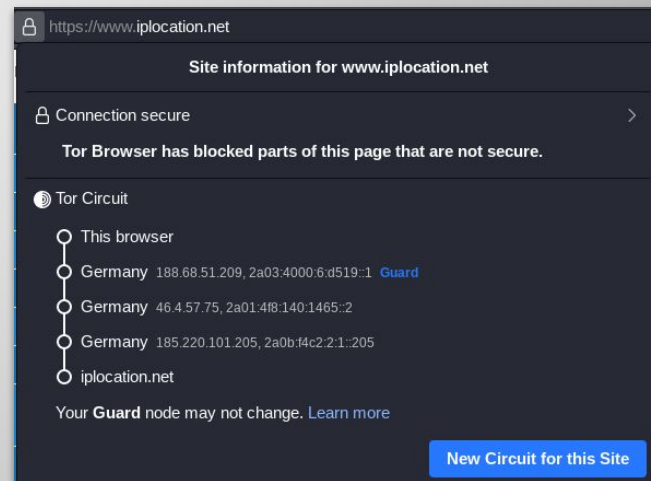
Коришћење TOR протокола



Како би открили ко стоји иза неког напада, форензичари морају пробити сваки слој од одредишта до излазног чвора да би утврдили нападача, што представља тежак процес. Још није развијен форензички алат који ово обезбеђује.

Пример 12. Коришћење TOR Browsera како би се обезбедила анонимност

```
$ tar -xf  
/home/kali/Documents/Dodatni_alati/tor-browser-linux64-  
11.0.13_en-US.tar.xz  
$ cd ~/Documents/Dodatni_alati/tor-browser_en-US  
$ ./start-tor-browser.desktop
```



СКРИВАЊЕ ТРАГОВА

- ЛАЖИРАЊЕ IP АДРЕСЕ
- ЛАЖИРАЊЕ MAC АДРЕСЕ
- МАНИПУЛАЦИЈА ЛОГ ДАТОТЕКАМА
- КОРИШЋЕЊЕ PROXY СЕРВЕРА И VPN-a
- КОРИШЋЕЊЕ THE ONION ROUTER (TOR) ПРОТОКОЛА
- КОРИШЋЕЊЕ ЗОМБИ НАЛОГА

Коришћење зомби налога

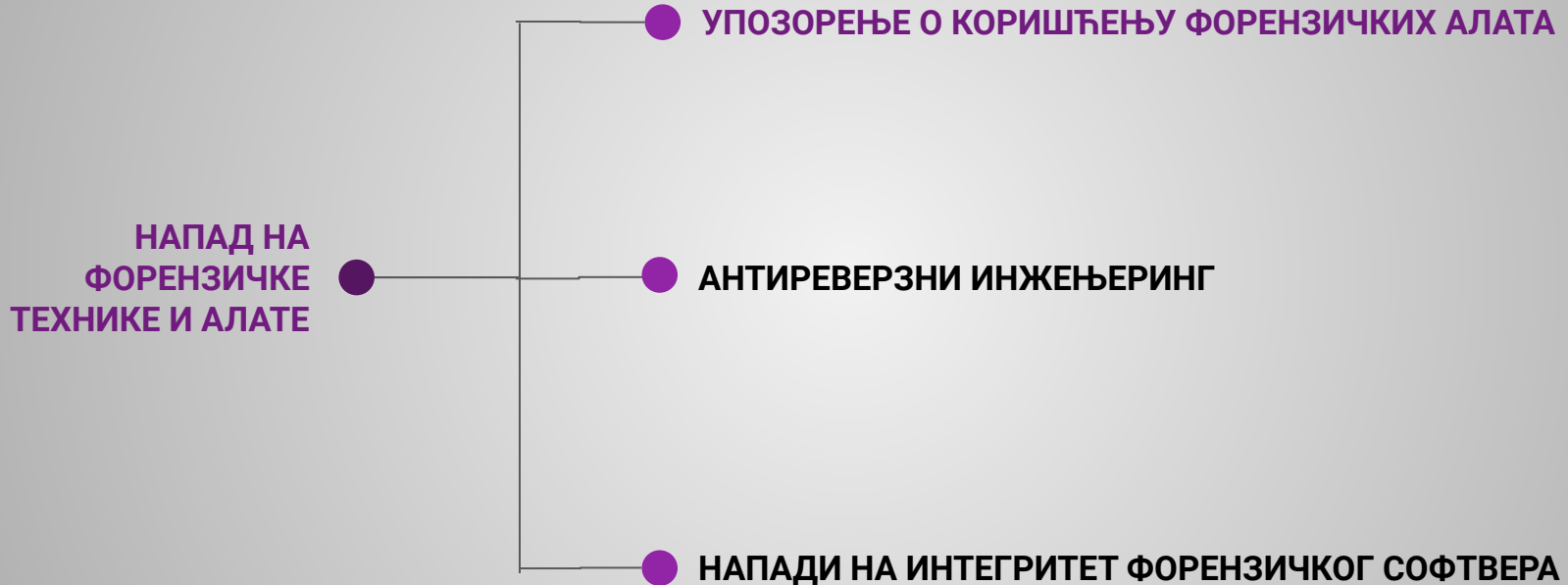
Налози које је неко користио и више не користи могу бити хаковани од стране трећег лица, који касније могу да их користе у неке злонамерне активности како би сакрили идентитет.

Спровођење злонамерних радњи са туђег рачунара или са туђе IP адресе.

Антифорензичке технике



Напад на форензичке технике и алате



Упозорење о коришћењу форензичких алата

Антивирусни програми могу да детектују форензичке алате и да покрену неке напредне технике брисања.

Пример: Уколико форензичар на упаљеном рачунару који има Windows оперативни систем жели да прикупи радну меморију, он ће инсталирати FTK Imager. Уколико постоји инсталиран антивирусни програм који може да детектује присуство овог форензичког алата, он ће покренути технике брисања рам меморије и тиме онемогућити прикупљање.

Напад на форензичке технике и алате



Антиреверзни инжењеринг

Реверзни инжењеринг је област која се бави реконструкцијом рада неког програма.

Уколико желимо да онемогућимо да неко може да изврши реконструкцију над нашим софтвером који развијамо, онда ћемо имплементирати одређене технике како бисмо онемогућили то. Те технике спадају под антиреверзни инжењеринг.

Напад на форензичке технике и алате



Напади на интегритет форензичког софтвера

Форензички софтвер као и сваки други софтвер може да има рањивости.

Могуће је искористити неку рањивост форензичког софтвера у оквиру свог уређаја како би онемогућили прикупљање података помоћу форензичког алата.

Препорука је да се форензичке истраге раде на посебној машини или VM.

Пример: Signal апликација за безбедну комуникацију је искористила рањивост Cellebrite алата за прикупљање меморије са мобилног уређаја. [Блог](#) са детаљима.



Факултет техничких наука
Лабораторија за дигиталну форензику

Now, you are a hacker!



Увод у дигиталну форензику
Јелена Драгишић, Светлана Антешевић