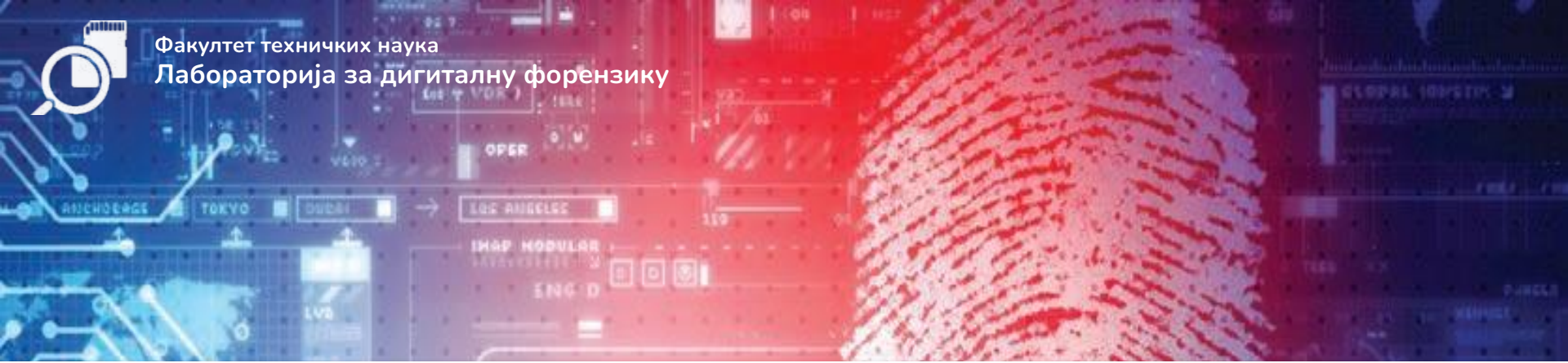


Факултет техничких наука
Лабораторија за дигиталну форензику

ФОРЕНЗИКА АПЛИКАЦИЈА

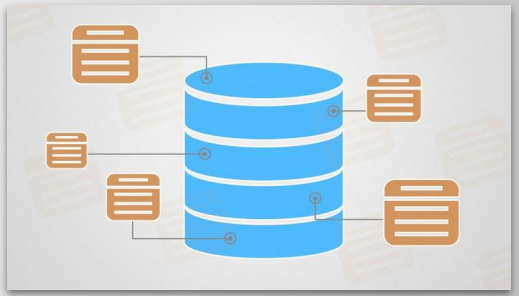
Увод у дигиталну форензику

Јелена Драгишић, Светлана Антешевић

Преглед области

Чиме се бави форензика апликација?

Форензика апликација је област дигиталне форензике чији предмет су дигитални докази настали као резултат рада апликација.



Напомена: мобилне апликације и мултимедијални записи ће се обрађивати на наредним терминима.

Преглед области

Којим дигитални докази су нам од значаја?

- ➔ Базе података апликација (sqlite, db, mdb ...)
- ➔ Документи и њихови метаподаци креирани од стране апликације (pdf, docx, txt, doc, ods, xls, csv, xml, html ...)
- ➔ Конфигурационе и лог датотеке одређене апликације (txt, xml ...)

Преглед области

Шта представља изазов?

- ➔ Велики број различитих апликација и верзија апликација
- ➔ Велики број различитих шема база података (чија спецификација често није доступна)
- ➔ Често апликација не складишти податке на уређају већ на неком удаљеном серверу, па је потребно обратити се компанији која је произвела апликацију за добијање података у одређеном периоду
- ➔ Велики број различитих формата докумената
- ➔ Постојање формата докумената које не можемо да интерпретирамо
- ➔ Метаподаци датотека се могу променити

Преглед области

Зашто је значајна?

Мноштво доказа произведених од стране корисника складишти се унутар база података и докумената који су настали као резултат рада апликације.

Ова област дигиталне форензике често је предмет вештачења.

Најчешће су то преваре путем неких од апликација за размену порука, банковних апликација или мејл клијената које комуницирају путем интернета.

Преглед области

Апликативни софтвер је рачунарски програм намењен извршавању задатака невезаних за функције оперативног система, инсталиран и намењен коришћењу од стране крајњих корисника.

Углавном складишти податке у базама података.

У зависности од намене софтвера може да произведе одређене датотеке које могу бити стандардизованог или специфікованог формата.

Преглед области

Подела апликативних софтвера

- ➔ Апликације за размену порука (Viber, WhatsApp, Messenger, Facebook, Telegram, Signal, Slack, TikTok, Skype ...)
- ➔ Мејл клијенти (Mozilla Thunderbird, Mailbird, Microsoft Outlook, Apple Mail, Google Mail ...)
- ➔ Наменске апликације за обрађивање слика, видеа, текста, кода.. (Photoshop, VSCode, PyCharm, Eclipse, Microsoft Office, Libre Office, Video Maker...)
- ➔ Веб претраживачи(Opera, Firefox, Chrome, Brave ...)
- ➔ Игрице, банковне апликације, канцеларијско пословање, финансијске апликације, забава и мноштво апликација других намена

Преглед области

База података је колекција података организованих за брзо претраживање и приступ.

Груба подела база података је на **SQL** (релационе) и **NoSQL** базе података (које немају формално спецификовану шему базе података).

Неке од SQL база података су: MySQL, Oracle DB, H2, SQLite, MS SQL ...

Неке од NoSQL база података по начину имплементације базе:

- Складишта података кључ-вредност (Riak, Voldemort)
- Колонски оријентисана (Cassandra, Hbase, SimpleDB)
- Документ оријентисана (MongoDB, CouchDB, RavenDB)
- Граф оријентисане (Neo4J, InfoGrid)
- XML базе података (eXist, Sedna, BaseX)

Преглед области

Базе података

Многе апликације чувају структуриране податке у релационим базама података и у ову сврху се често користи SQLite (уграђени систем за управљање базама података).

Чести формати датотека су: sqlite, db, mdb ...

Ови подаци могу да се прегледају коришћењем различитих апликација (које зависе од система за управљање базама податка).

За задавање упита ка бази података потребно је претходно познавање шеме базе података или начина организовања, упитног језика (SQL, jQuery, MQL(MongoDB Query Language) ...), као и параметара за приступ(нпр. лозинка).

Преглед области

Датотека или фајл је структурирани скуп података садржајно везаних, смештених на медију за меморисање.

Формати датотека стандарди који специфицирају како се кодирају информације у датотекама. Могу се грубо поделити на текстуалне формате и бинарне формате.

Формат датотеке може се одредити на основу екстензије датотеке, заглавља датотеке (тзв. магичног броја) или екстерних метаподатака

Магични број или потпис документа генерално означава тип датотеке и везују се за одређену екстензију документа, док тип датотеке нема увек дати магични број.

Преглед области

Магични број или потпис документа

```
25 50 44 46                    %PDF
```

PDF, FDF, AI — Adobe Portable Document Format, Forms Document Format, and Illustrator graphics files

Trailers:

```
0A 25 25 45 4F 46 (.%%EOF)
0A 25 25 45 4F 46 0A (.%%EOF.)
0D 0A 25 25 45 4F 46 0D 0A (..%%EOF..)
0D 25 25 45 4F 46 0D (.%%EOF.)
```

NOTE: There may be multiple end-of-file marks within the file. When carving, be sure to get the last one.

```
50 4B 03 04 14 00 06 00        PK......
```

DOCX, PPTX, XLSX — Microsoft Office Open XML Format (OOXML) Document

NOTE: There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the <*Override PartName*= tag, where you will find *word*, *ppt*, or *xl*, respectively.

Trailer: Look for `50 4B 05 06` (`PK..`) followed by 18 additional bytes at the end of the file.

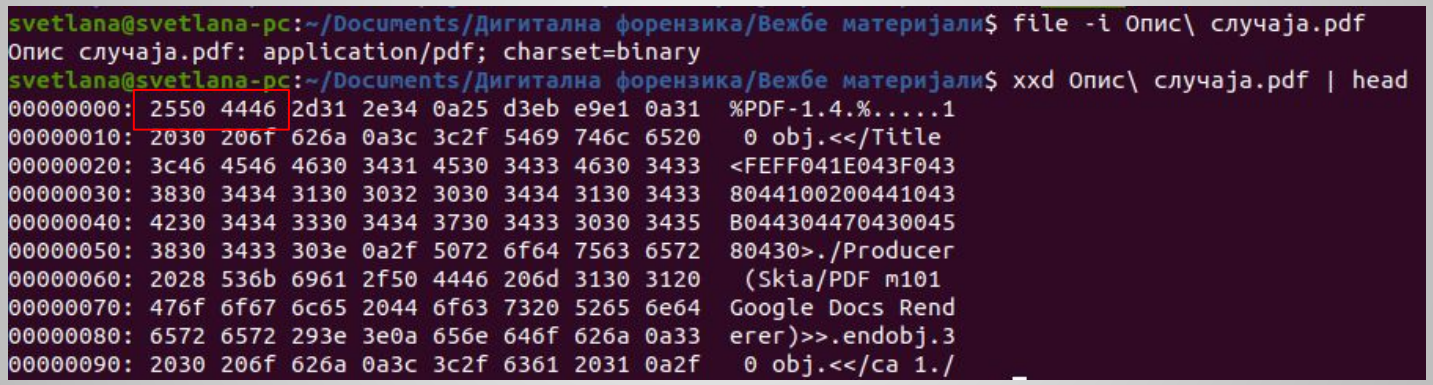
```
53 51 4C 69 74 65 20 66        SQLite f
6F 72 6D 61 74 20 33 00        ormat 3.
```

DB — SQLite database file

Преглед области

Магични број или потпис документа

Ако користите Linux/MacOS/Unix систем, можете користити команду датотеке да бисте одредили тип датотеке на основу потписа датотеке, према магичној датотеци система.



Додатни детаљи о форматима графичких датотека као и аудио и видео датотека могу се наћи на Формати графичких датотека и на страници Планирање одрживости дигиталних формата. Док други магични бројеви формата могу се наћи на интернету.

Преглед области

Апликације за канцеларијско пословање

Резултат рада апликација за канцеларијско пословање су документи у различитим форматима (који зависе од апликације)

Документима могу да буду придружени и метаподаци (чија шема зависи од типа документа)

Текстуални документи:

- Microsoft Office Format (doc/docx)
- Open Document Format Text (odt)
- Rich Text Format (rtf)
- Portable Document Format (PDF)
- HyperText Markup Language (HTML)

Преглед области

Апликације за канцеларијско пословање

Унакрсне табеле:

- Microsoft Office Format (xls/xlsx)
- Open Document Format Spreadsheet (ods)

Остали типови докумената: презентације, цртежи, математичке формуле, календари, листе задатака, именици ...

Метаподаци - се обично складиште као парови (кључ, вредност). Синтакса и семантика метаподатака одређена је шемом метаподатака. Шеме метаподатака зависе од типа документа.

Преглед области

Интернет или веб прегледачи

Током рада производе различите артефакте.

Ти артефакти се обично складиште у SQLite базама података (структурирани подаци) или у датотекама (неструктурирани подаци).

Локација база података и датотека варира у зависности од апликације и оперативног система.

Преглед области

Интернет или веб прегледачи - артефакти

- ➔ History
- ➔ Cache
- ➔ Cookies
- ➔ Typed URLs
- ➔ Sessions
- ➔ Most visited sites
- ➔ Screenshots
- ➔ Financial info
- ➔ Form values (Searches, Autofill)
- ➔ Downloaded files (Downloads)
- ➔ Favorites

Преглед области

Апликације за рад са електронском поштом

Чувају локалне копије поштанских сандучића и конфигурационе параметре потребне за повезивање на SMTP/POP3/IMAP и Exchange сервере.

- ➔ Microsoft Exchange сервери: Outlook Data File (.pst), Offline Outlook Data File (.ost)
- ➔ POP3/IMAP сервери: Mbox, Maildir

Формати поштанских сандучића варирају у зависности од апликације.

Локација поштанских сандучића и конфигурационих датотека варирају у зависности од апликације и оперативног система.

Формат електронских писама прописан је **IETF RFC 5322** стандардом

Процес форензичке истраге

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

Прегледање и анализа

Припрема и екстракција потенцијалних доказа из прикупљених извора података ради даље анализе.

Бавићемо се анализом апликација:

- Веб претраживач Opera 36.0
- Веб претраживач Firefox 66.0.3
- Мејл клијент Mozilla Thunderbird 91.8.1

Прегледање и анализа

Autopsy & The Sleuth Kit - ingest модули:

- **Recent Activity** - издваја корисничку активност у последњих 7 дана коју чувају веб претраживачи, инсталирани програми и оперативни систем.
- **File Type Identification** - идентификује датотеке на основу њихових интерних потписа и не ослања се на екстензије датотека. Многи модули зависе од резултата овог модула.
- **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).
- **Email Parser** - идентификује Thunderrbird MBOX датотеке и PST формате датотека на основу потписа датотека, издваја е-поруке из њих, додаје прилоге као изведене датотеке.

Прегледање и анализа

DB Browser for SQLite

Софтверски алат који служи за прегледање и анализу SQLite база података.

Омогућава да истражите датотеке базе података са следећим екстензијама: .sqlite, .sqlite3, .sqlitedb, .db, и .db3.

Прегледање и анализа

Веб претраживач Opera 36.0

Локације датотека:

- **Win XP:** C:\Documents and Settings\$USER\Application Data\Opera Software\Opera Stable
- **Win XP:** C:\Documents and Settings\$USER\Local Settings\Application Data\Opera Software\Opera Stable
- **Linux**: /home/$USER/.opera/
- **MacOS**: /Users/$USER/Library/Opera/

Прегледање и анализа

Веб претраживач Opera 36.0

Датотеке од значаја:

- **Bookmarks** - Информације о обележивачима се чувају у овој текстуалној датотеци. Занимљиве информације: name, created timestamp, visited timestamp, url.
- **Cookies** - Колачићи које је корисник омогућио ради прикупљања статистичких информација одређених веб сајтова. Могу да садрже информације о кориснику и његовим подешавањима за одређени сајт. У оквиру ове датотеке чувају се информације о називу колачића, сајт који га је креирао, времену креирања, времену истека, путањи..
- **History** - датотека која чува историју прегледања, url од посећених сајтова, download податке...
- **Preferences** - датотека која садржи у json формату корисничке дозволе за оређене сајтове.
- **Web Data** - датотека која чува податке о autofill пољима, credit cards, keywords..

Прегледање и анализа

Веб претраживач Firefox 66.0.3

Локације датотека:

- **Linux**: /home/$USER/.mozilla/firefox/$PROFILE.default/
- **Win XP:** C:\Documents and Settings\$USER\Application Data\Mozilla\Firefox\Profiles\$PROFILE.default\
- **Win**: C:\Users\$USER\AppData\Roaming\Mozilla\Firefox\Profiles\$PROFILE.default
- **MacOS**: /Users/$USER/Library/Application Support/Firefox/Profiles/$PROFILE.default/

Прегледање и анализа

Веб претраживач Firefox 66.0.3

Датотеке од значаја:

- ➔ **webappstore.sqlite** - ова датотека складишти све токене из XAuth, главна идеја XAuth-a је да ће декларисани токен бити доступан само са XAuth.org домена за који је подешен.
- ➔ **places.sqlite** - база података посећених места, обележивача, атрибута за оне сајтове које обично посећује претраживач. Омогућава истраживачу да извуче целокупну веб историју за корисника.
- ➔ **permissions.sqlite** - ово је историја тога која веб локација има које дозволе, на пример дозвољавање или не дозвољавање искачућих прозора, или сајтова који имају повезане акредитиве за куповину.
- ➔ **formhistory.sqlite** - ово је историја сваког обрасца који сте икада попунили на мрежи, од е-поште до каталога, све је у овој датотеци.

Прегледање и анализа

Веб претраживач Firefox 66.0.3

Датотеке од значаја:

- ➔ **extensions.json** и **extensions.ini** - сва проширења веб претраживача
- ➔ **cookies.sqlite** - ово је спремиште сваког колачића који поставља систем, ово може, али не мора бити потпуно очишћено када корисник избрише све колачиће, или користећи програм као што је CCleaner за брисање колачића
- ➔ **content-prefs.sqlite** - Сврха ове функције је да омогући корисницима да поставе преференце за претраживач и поставке садржаја (тј. зумирање текста, стил странице и кодирање знакова) на бази специфичној за сајт уместо само на основу картице или странице , и да задржи та подешавања током посета страницама и сесија прегледања, како би се побољшала корисност тих подешавања. Ово је добра датотека за форензичку анализу јер приказује сајтове који се редовно користе, од којих неки корисник можда не зна да се чувају.

Прегледање и анализа

Веб претраживач Firefox 66.0.3

Датотеке од значаја:

- ➔ **downloads.json** - база података сваке преузете датотеке.
- ➔ **addons.json -** сви додаци претраживача и други подаци о томе ко може да их користи у окружењу са више профила.

Прегледање и анализа

Мејл клијент Mozilla Thunderbird 91.8.1

Апликација за е-пошту која је развијена од стане Mozilla фондације.

Локације датотека:

- **Linux**: /home/$USER/.thunderbird/firefox/$PROFILE.default-release/
- **Win XP:** C:\Documents and Settings\$USER\Application Data\Thunderbird\Profile\
- **Win**: C:\Users\$USER\AppData\Roaming\Thunderbird\Profile\
- **MacOS**: /Users/$USER/Library/Application Support/Thunderbird/Profile/

Прегледање и анализа

Мејл клијент Mozilla Thunderbird 91.8.1

Датотеке од значаја:

- ➔ **abook.sqlite** - садржи информације о датотеци history.mab, што је скраћеница од Mozilla Address Book. MAB чува личне и пословне контакт информације као што су: име, презиме, мејл адреса, адреса становања, подаци о радном месту..
- ➔ **cookies.sqlite -** ово је спремиште сваког колачића који поставља систем, ово може, али не мора бити потпуно очишћено када корисник избрише све колачиће, или користећи програм као што је CCleaner за брисање колачића
- ➔ **extensions.json** - чува сва проширења апликације
- ➔ **favicons.sqlite -** чува све мале иконе повезане са одређеном е-поштом, URL датотеке, MIME тип, датум и време истека.
- ➔ **formhistory.sqlite** - ово је историја сваког обрасца који сте икада попунили на мрежи, од е-поште до каталога, све је у овој датотеци.

Прегледање и анализа

Мејл клијент Mozilla Thunderbird 91.8.1

Датотеке од значаја:

- **global-messages-db.sqlite -** представља глобалу базу података која садржи информације о систему за индексирање који се користи за претрагу порука, CC, BCC email, DB message ID, header message ID, attachments, from, to, subject, message body, is read, is replied, is starred, is forwarded, is encrypted..
- **places.sqlite -** садржи информације о обележивачима, историји уноса, кључним речима, историји прегледања и везама на које је кликнуто у порукама поште.
- **ImapMail -** фолдер који садржи сачуван inbox, drafts, archives, sent, templates имејл порука у msf формату који је специфичан за Thunderbird апликаицју.
- **Mail/Local Folders** - фолдер који садржи trash, unsent messages у msf формату.

Прегледање и анализа докумената

За прегледање и анализу докумената можемо користити алат који је спецификован за тражени формат документа.

Пример pdf документ:

- Садржају pdf документа можемо приступити помоћу било ког претраживача, pdf viewer-а или edior-а као и помоћу Autopsy алата.
- Метаподатке pdf документа можемо увидети у оквиру properties документа, као и помоћу неких од алата: exiftool, Autopsy...

  $ exiftool nazivfajla.pdf

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.

Корисни линкови и книге

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