COMPUTER FORENSIC AND INVESTIGATION

16BCA5CD11

Credits: 4

(ISMA) – 5th SEM

Module-4

Forensics Techniques-II

LECTURE : 4

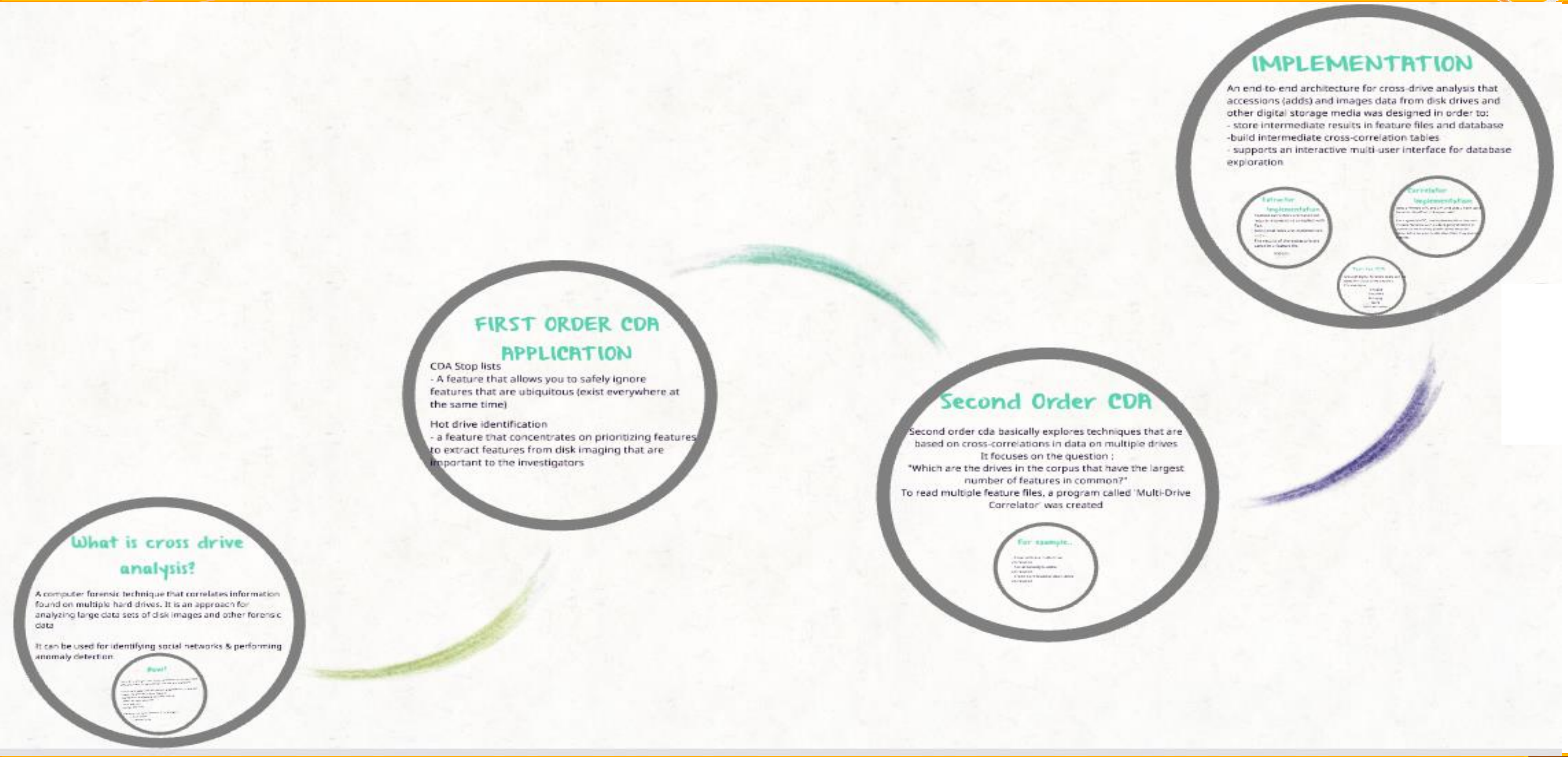
PRACTICAL: 0

TUTORIAL : 0

Ajay Shriram Kushwaha

DISCIPLINE SPECIFIC ELECTIVE (DSE) - 2

Cross Drive Analysis



What is cross drive analysis?

A computer forensic technique that correlates information found on multiple hard drives. It is an approach for analyzing large data sets of disk images and other forensic data

It can be used for identifying social networks & performing anomaly detection

How?

FIRST ORDER CDA APPLICATION

CDA Stop lists
- A feature that allows you to safely ignore features that are ubiquitous (exist everywhere at the same time)

Hot drive identification
- a feature that concentrates on prioritizing features to extract features from disk imaging that are important to the investigators

Second Order CDA

Second order cda basically explores techniques that are based on cross-correlations in data on multiple drives
It focuses on the question :
"Which are the drives in the corpus that have the largest number of features in common?"
To read multiple feature files, a program called 'Multi-Drive Correlator' was created

For example..

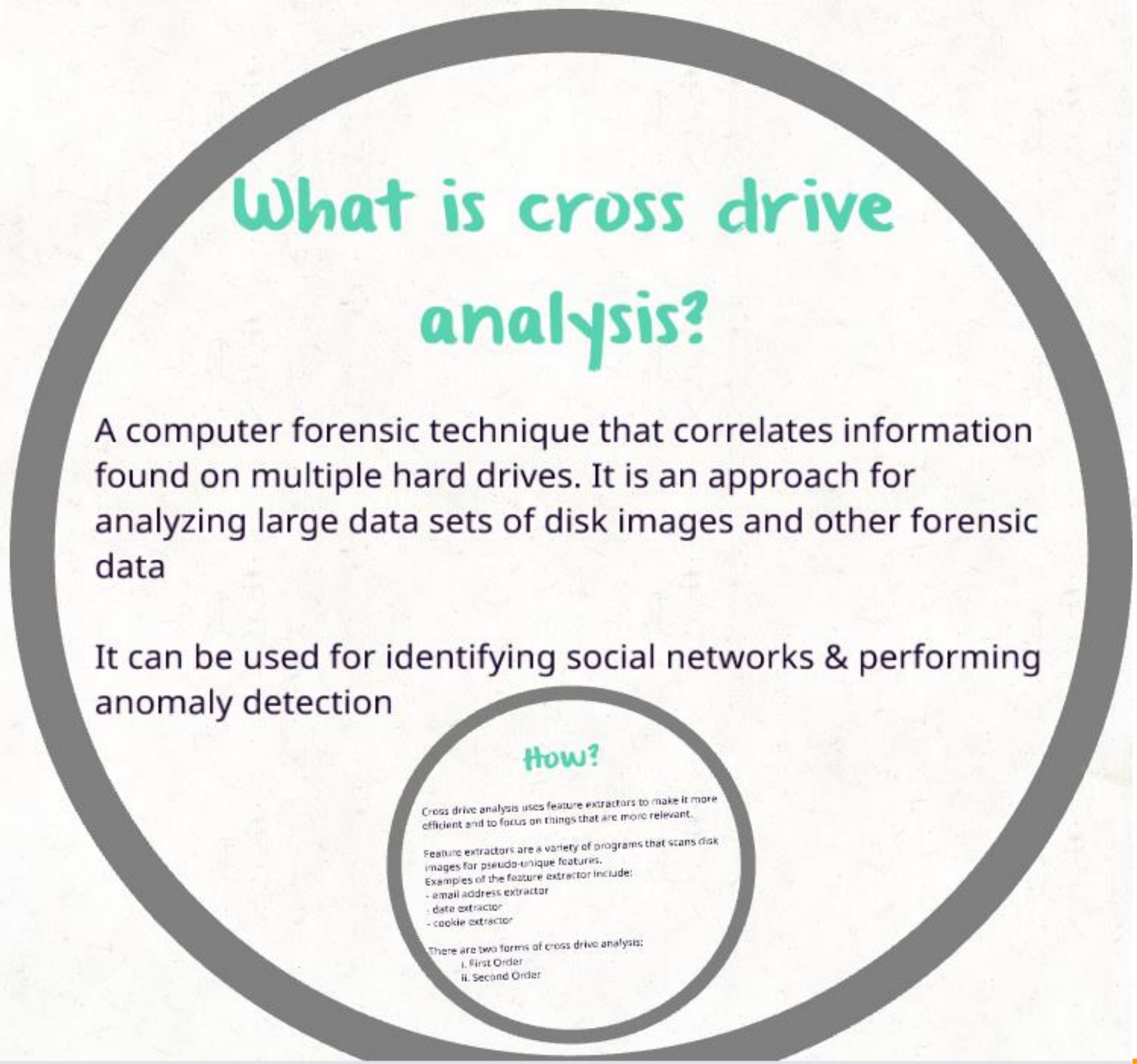
IMPLEMENTATION

An end-to-end architecture for cross-drive analysis that accessions (adds) and images data from disk drives and other digital storage media was designed in order to:
- store intermediate results in feature files and database
-build intermediate cross-correlation tables
- supports an interactive multi-user interface for database exploration

Extractor Implementation

Correlator Implementation

Cross Drive Analysis



What is cross drive analysis?

A computer forensic technique that correlates information found on multiple hard drives. It is an approach for analyzing large data sets of disk images and other forensic data

It can be used for identifying social networks & performing anomaly detection

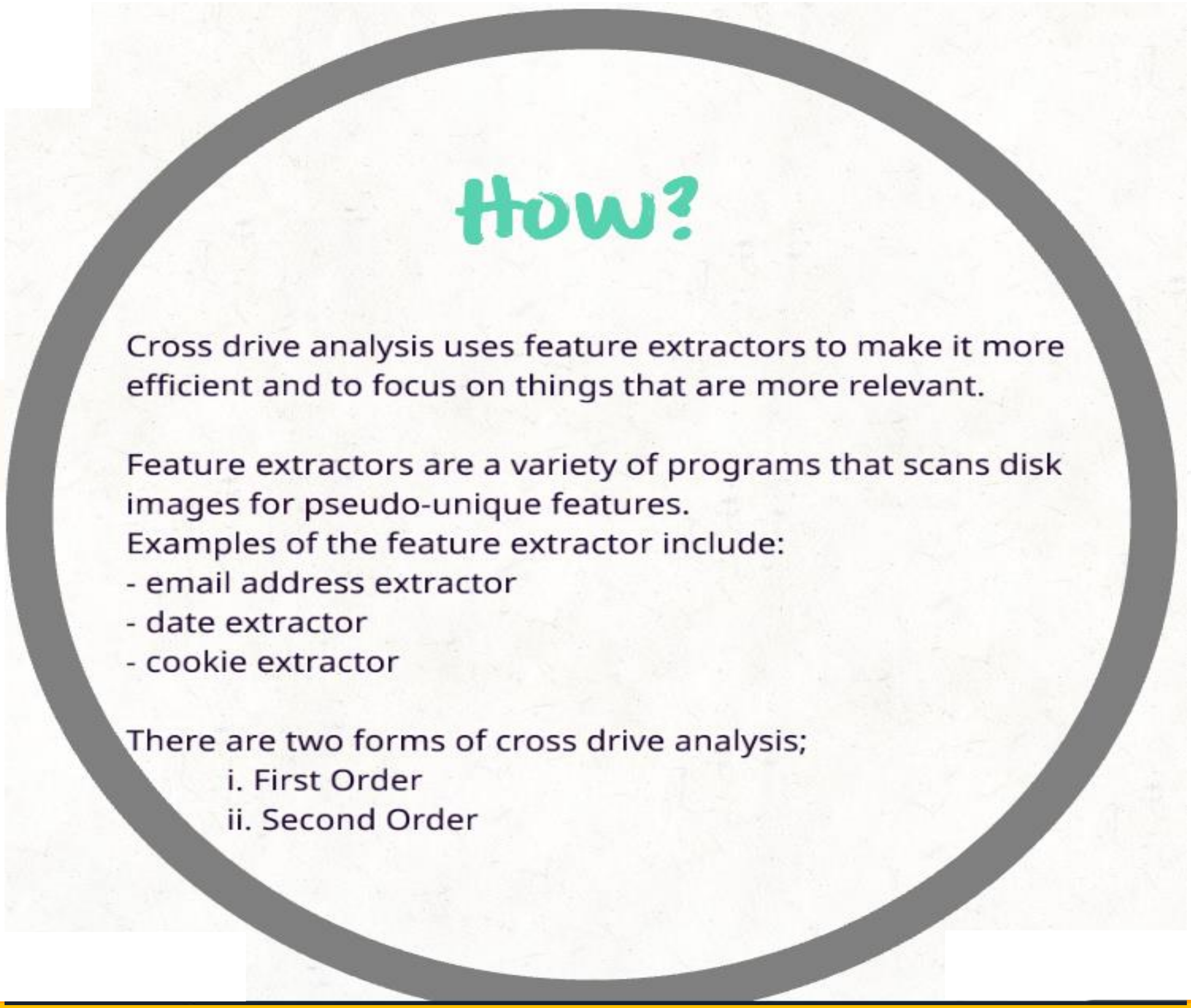
How?

Cross drive analysis uses feature extractors to make it more efficient and to focus on things that are more relevant.

Feature extractors are a variety of programs that scans disk images for pseudo-unique features.
Examples of the feature extractor include:
- email address extractor
- date extractor
- cookie extractor

There are two forms of cross drive analysis:
i. First Order
ii. Second Order

Cross Drive Analysis



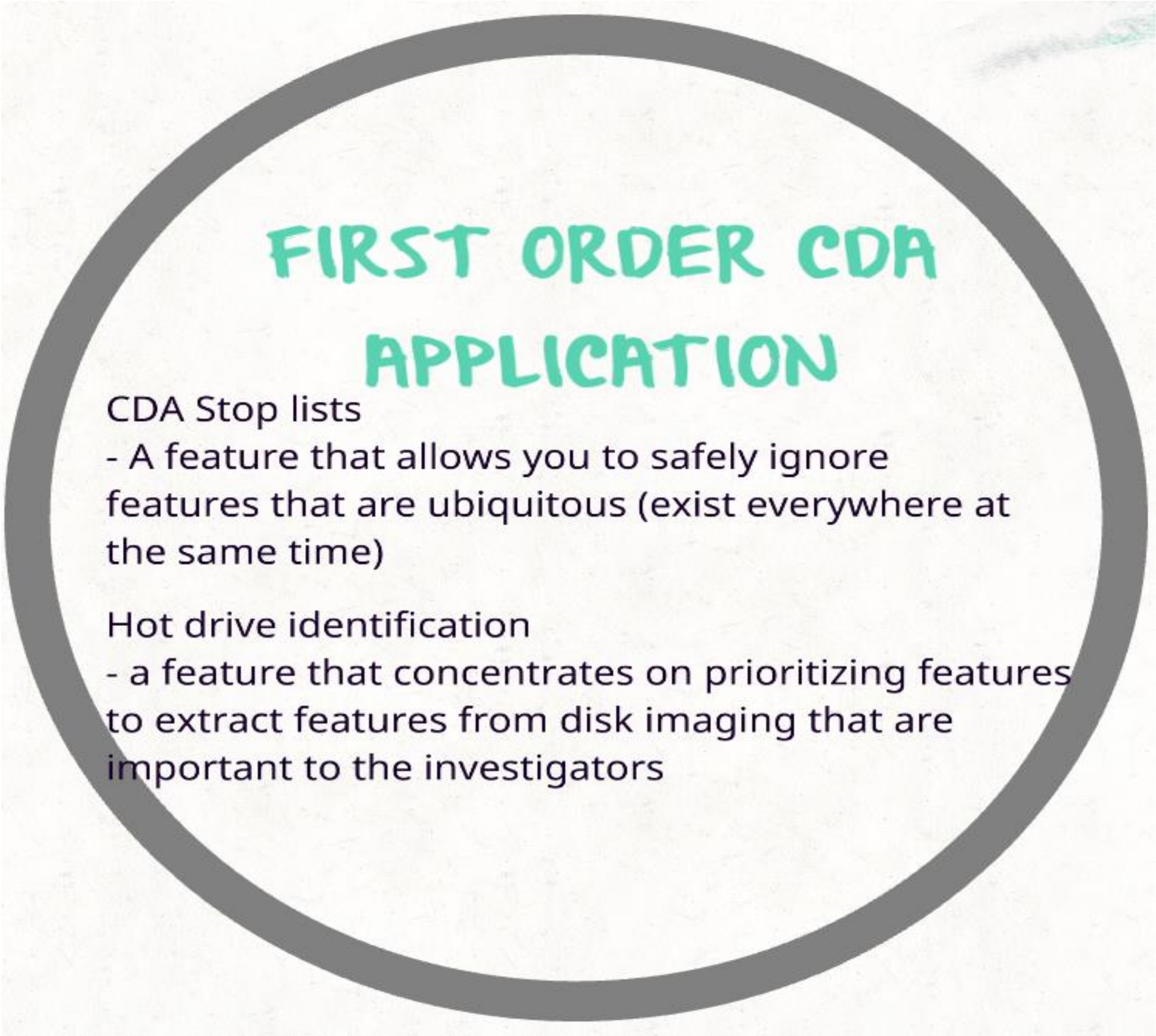
How?

Cross drive analysis uses feature extractors to make it more efficient and to focus on things that are more relevant.

Feature extractors are a variety of programs that scans disk images for pseudo-unique features.
Examples of the feature extractor include:
- email address extractor
- date extractor
- cookie extractor

There are two forms of cross drive analysis;
i. First Order
ii. Second Order

Cross Drive Analysis

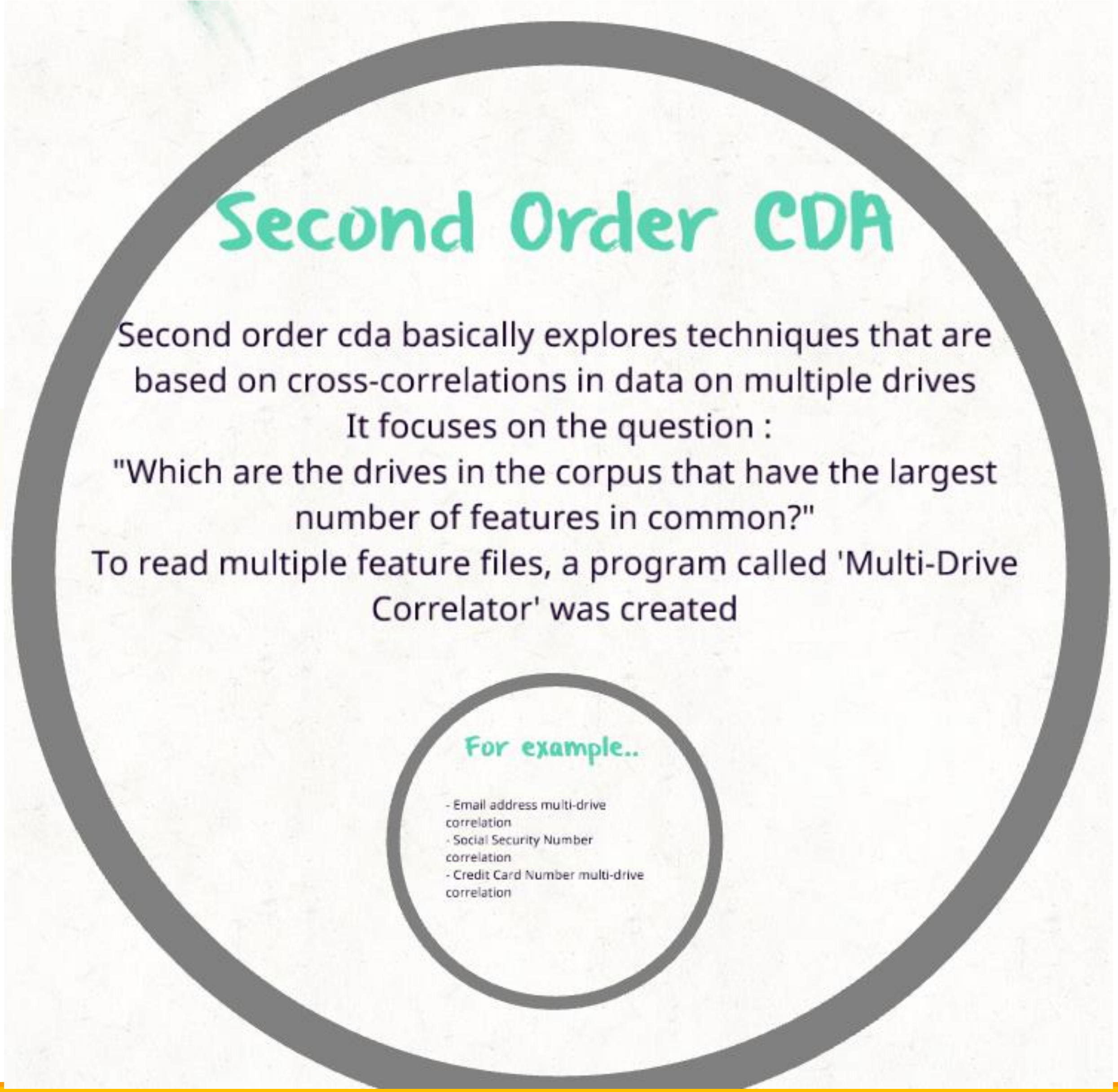


FIRST ORDER CDA APPLICATION

CDA Stop lists
- A feature that allows you to safely ignore features that are ubiquitous (exist everywhere at the same time)

Hot drive identification
- a feature that concentrates on prioritizing features to extract features from disk imaging that are important to the investigators

Cross Drive Analysis



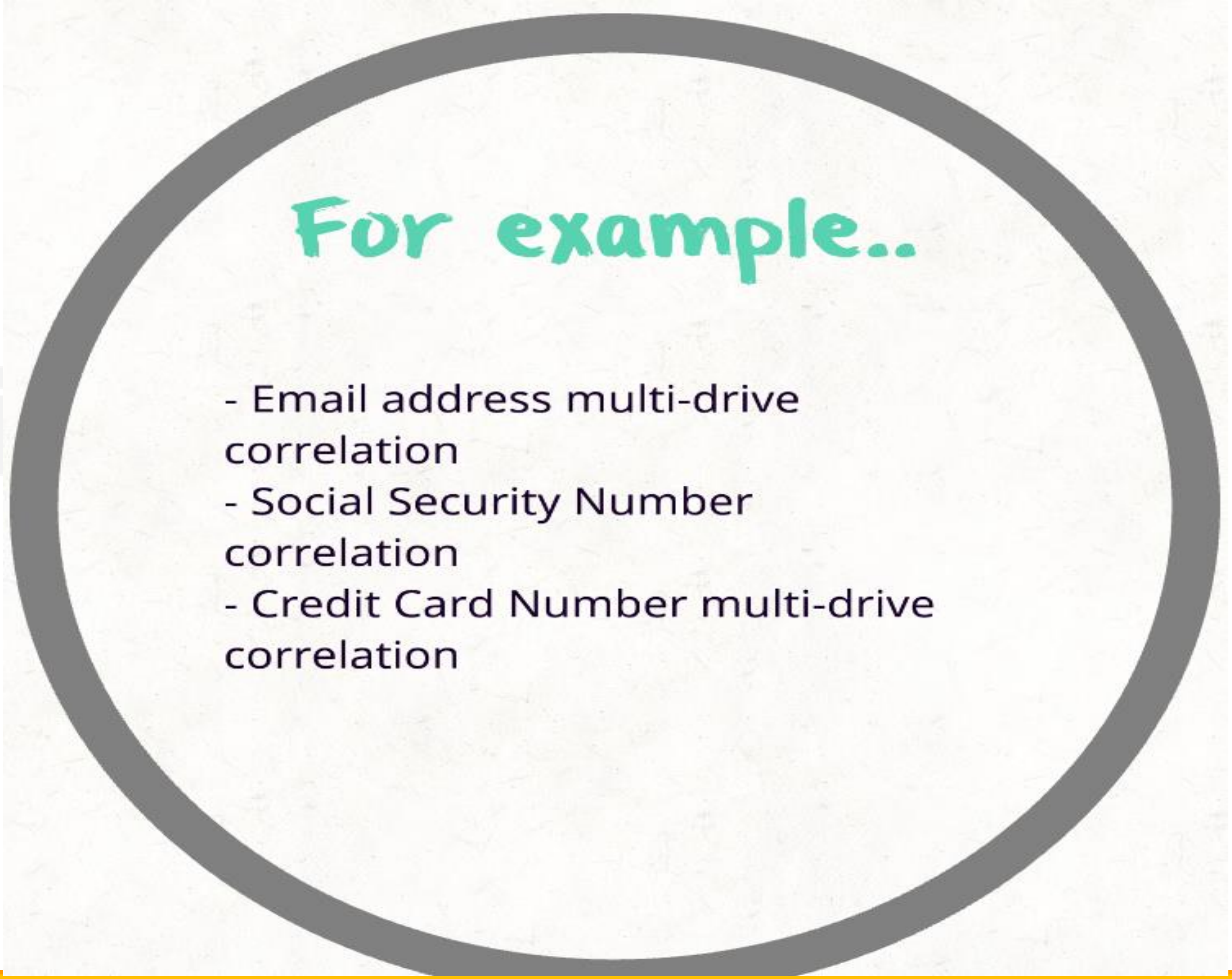
Second Order CDA

Second order cda basically explores techniques that are based on cross-correlations in data on multiple drives
It focuses on the question :
"Which are the drives in the corpus that have the largest number of features in common?"
To read multiple feature files, a program called 'Multi-Drive Correlator' was created

For example..

- Email address multi-drive correlation
- Social Security Number correlation
- Credit Card Number multi-drive correlation

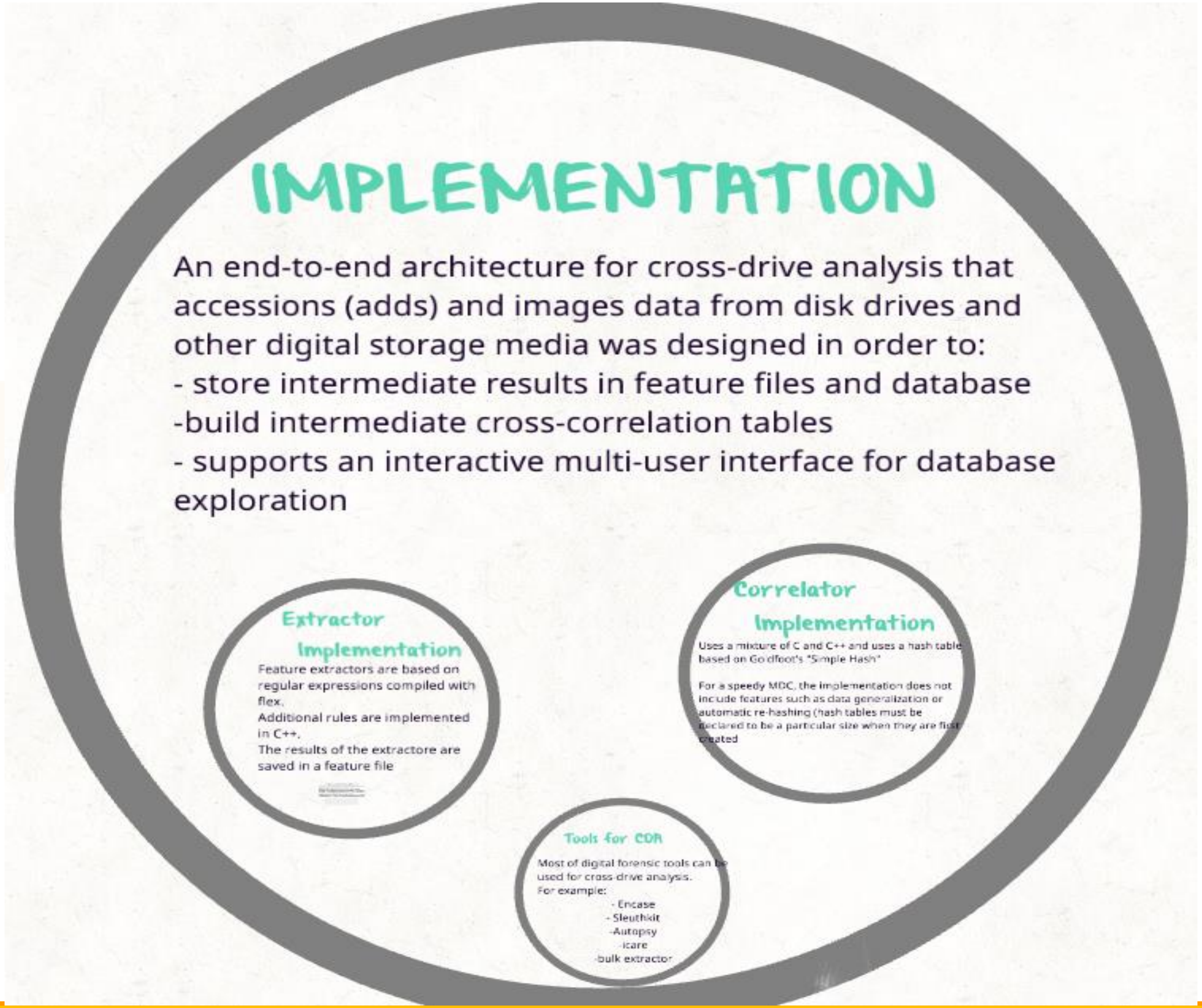
Cross Drive Analysis



For example..

- Email address multi-drive correlation
- Social Security Number correlation
- Credit Card Number multi-drive correlation

Cross Drive Analysis



IMPLEMENTATION

An end-to-end architecture for cross-drive analysis that accessions (adds) and images data from disk drives and other digital storage media was designed in order to:
- store intermediate results in feature files and database
-build intermediate cross-correlation tables
- supports an interactive multi-user interface for database exploration

Extractor Implementation

Feature extractors are based on regular expressions compiled with flex.
Additional rules are implemented in C++.
The results of the extractore are saved in a feature file

Correlator Implementation

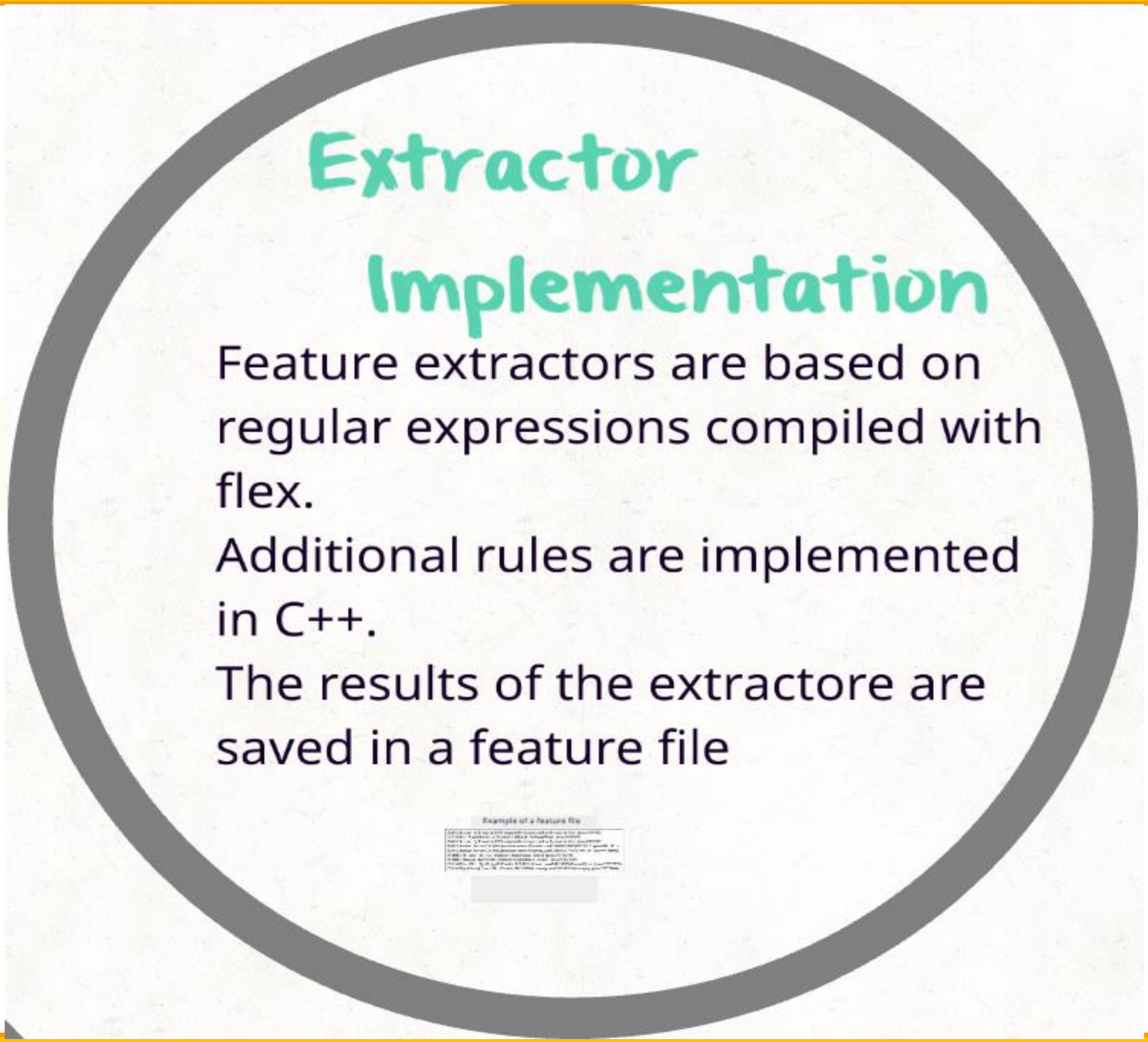
Uses a mixture of C and C++ and uses a hash table based on Go dfoot's "Simple Hash"

For a speedy MDC, the implementation does not include features such as data generalization or automatic re-hashing (hash tables must be declared to be a particular size when they are first created

Tools for CDA

Most of digital forensic tools can be used for cross-drive analysis.
For example:
- Encase
- Sleuthkit
-Autopsy
-icare
-bulk extractor

Cross Drive Analysis



Extractor Implementation

Feature extractors are based on regular expressions compiled with flex.

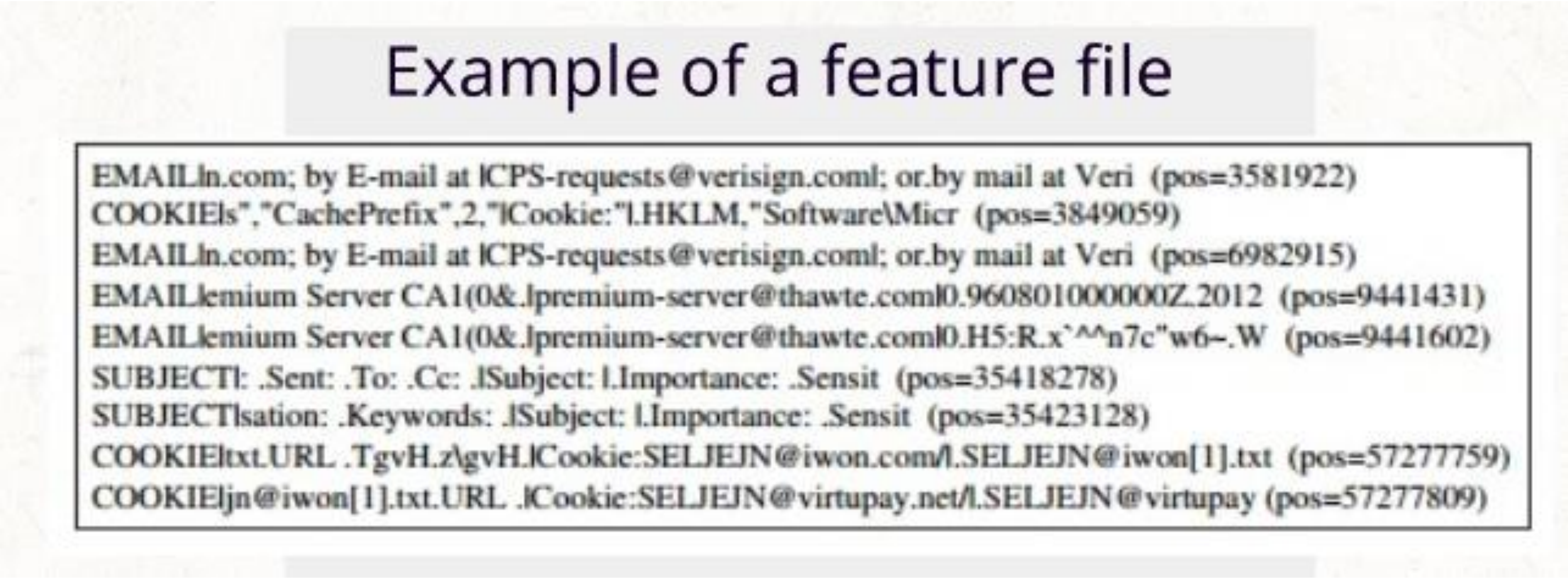
Additional rules are implemented in C++.

The results of the extractore are saved in a feature file

Example of a feature file

```
[illegible]
```

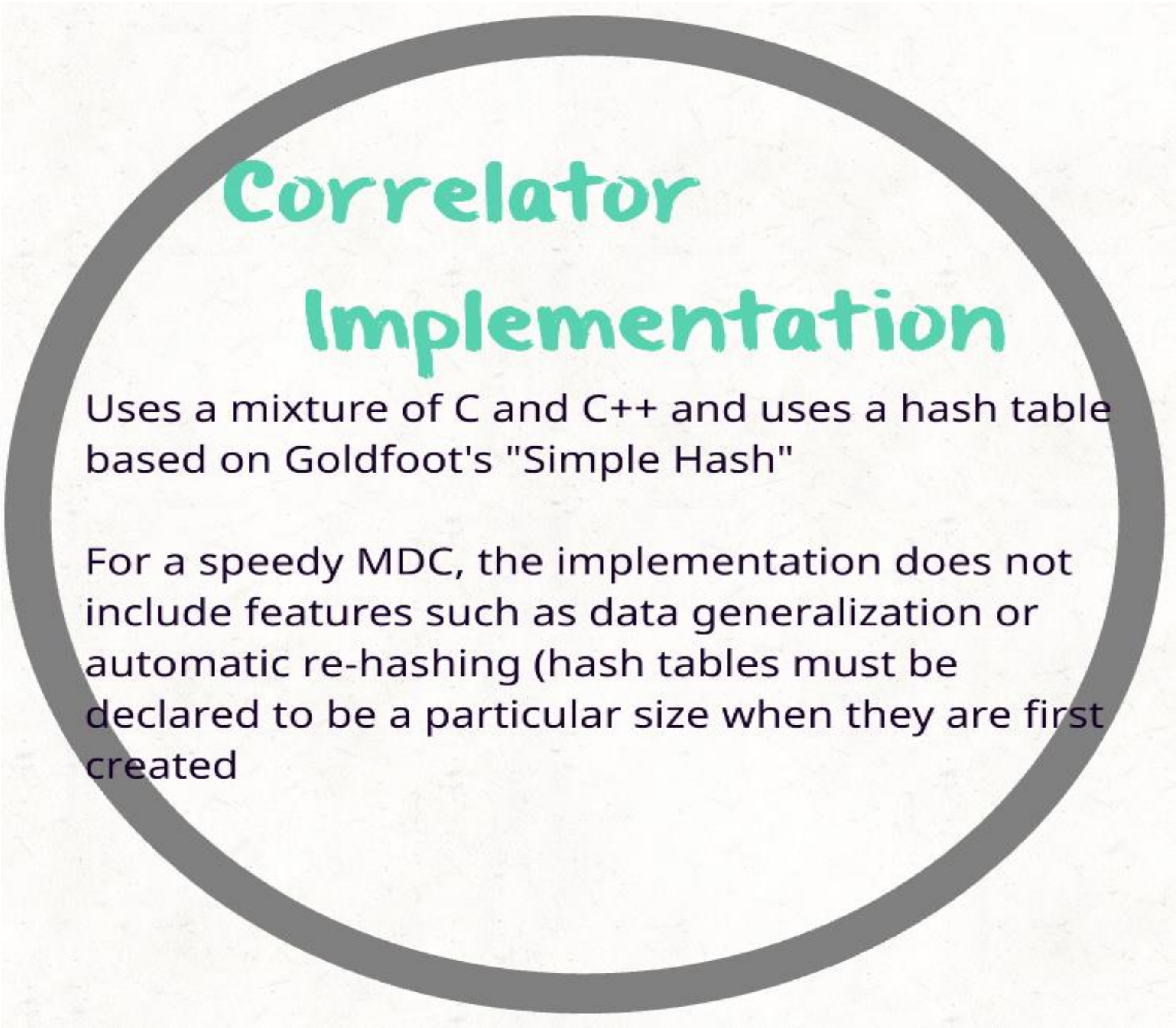
Cross Drive Analysis



Example of a feature file

```
EMAILln.com; by E-mail at lCPS-requests@verisign.coml; or.by mail at Veri  (pos=3581922)
COOKIEls","CachePrefix",2,"lCookie:"l.HKLM,"Software\Micr  (pos=3849059)
EMAILln.com; by E-mail at lCPS-requests@verisign.coml; or.by mail at Veri  (pos=6982915)
EMAILlemium Server CA1(0&.lpremium-server@thawte.coml0.960801000000Z.2012  (pos=9441431)
EMAILlemium Server CA1(0&.lpremium-server@thawte.coml0.H5:R.x`^^n7c"w6~.W  (pos=9441602)
SUBJECTl: .Sent: .To: .Cc: .lSubject: l.Importance: .Sensit  (pos=35418278)
SUBJECTlsation: .Keywords: .lSubject: l.Importance: .Sensit  (pos=35423128)
COOKIEltxt.URL .TgvH.z\gvH.lCookie:SELJEJN@iwon.com/l.SELJEJN@iwon[1].txt  (pos=57277759)
COOKIEljn@iwon[1].txt.URL .lCookie:SELJEJN@virtupay.net/l.SELJEJN@virtupay (pos=57277809)
```

Cross Drive Analysis

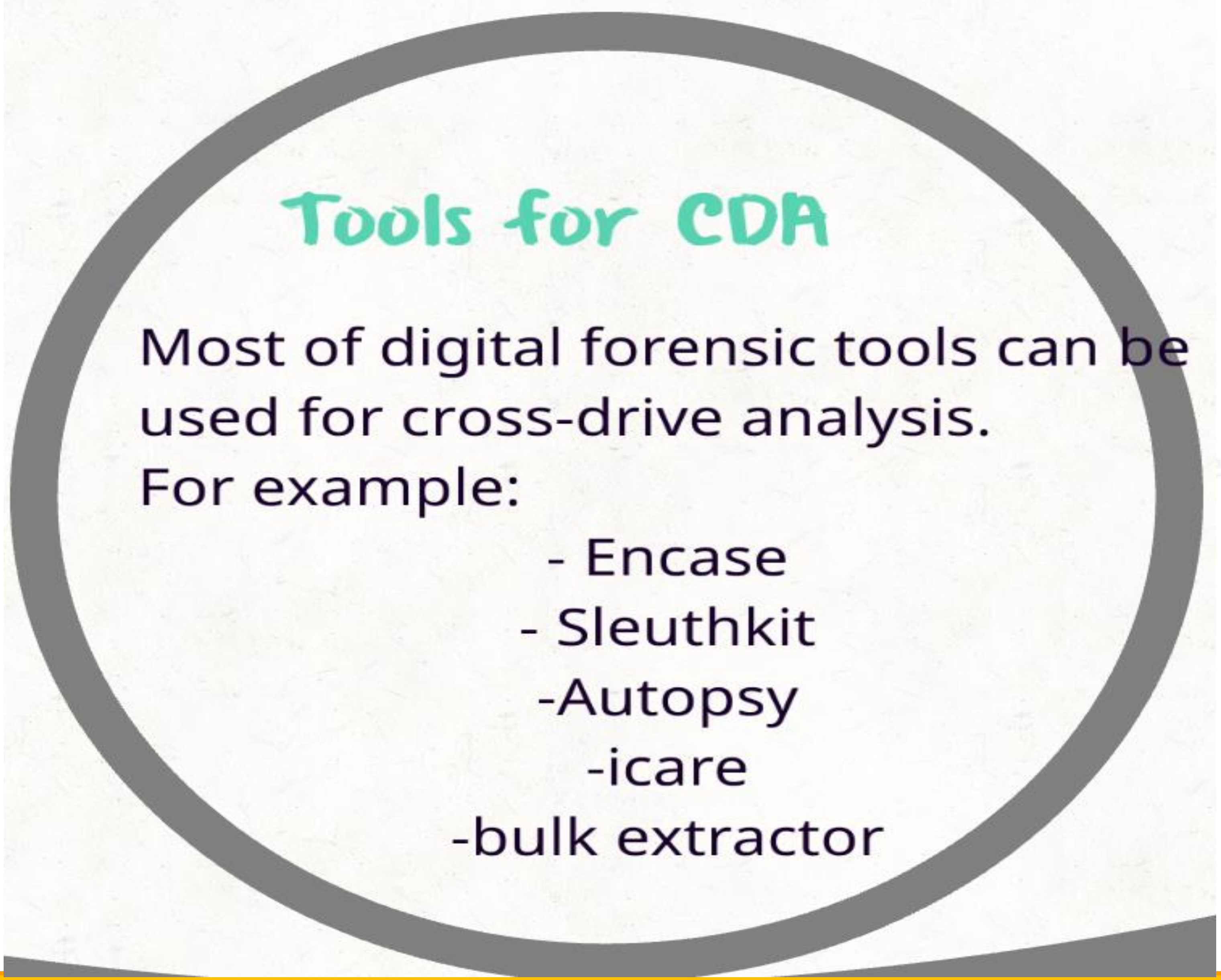


Correlator Implementation

Uses a mixture of C and C++ and uses a hash table based on Goldfoot's "Simple Hash"

For a speedy MDC, the implementation does not include features such as data generalization or automatic re-hashing (hash tables must be declared to be a particular size when they are first created

Cross Drive Analysis



Tools for CDA

Most of digital forensic tools can be used for cross-drive analysis.

For example:

- Encase
- Sleuthkit
-Autopsy
-icare
-bulk extractor

Live Analysis

- Gathers data from system during operation

Approaches:

- **Using standard user interface** : OS GUI,Command Shell, Secure Shell & Telnet

  Obtain Information : Current users, Open ports, n/w connections and Ps list

- **Using imported utilities**: Perform live analysis using tools but not directly installed on to the target machine. i.e., By using CD-ROM to access via command directory to do the investigation.

- **Using a modified system**: By using Honeypot or Honey net deployed as an intermediary to gather all the information to do the investigation.

- **Using additional hardware**: To copy the portions of memory from a running system. Using an hardware devices attached to an System buses such as PCI or Firewire bus to monitor the process.

Why Dictionary Attacks

What are the goals?

- Identify accounts configured with weak or default passwords – “It’s human nature”
- Use accounts as *entry points during penetration tests*

What’s the impact?

- Unauthorized access to critical:

  –*Systems*

  –*Applications*

  –*data*

- User impersonation

Are There Alternatives

Yes.

- **Approaches typically includes:**

Cracking pw hashes offline with:

–Pre-computed hash libraries like *Rainbow Tables*

–Brute force and dictionary techniques using tools like *Hashcat and John the Ripper*

- Dumping clear text passwords for interactive sessions with *Mimikatz*

Dictionary Attacks: Process

Windows Dictionary Attack Process

1.Identify domains

2.Enumerate domain controllers (servers which respond to security authentication requests)

3.Enumerate domain users

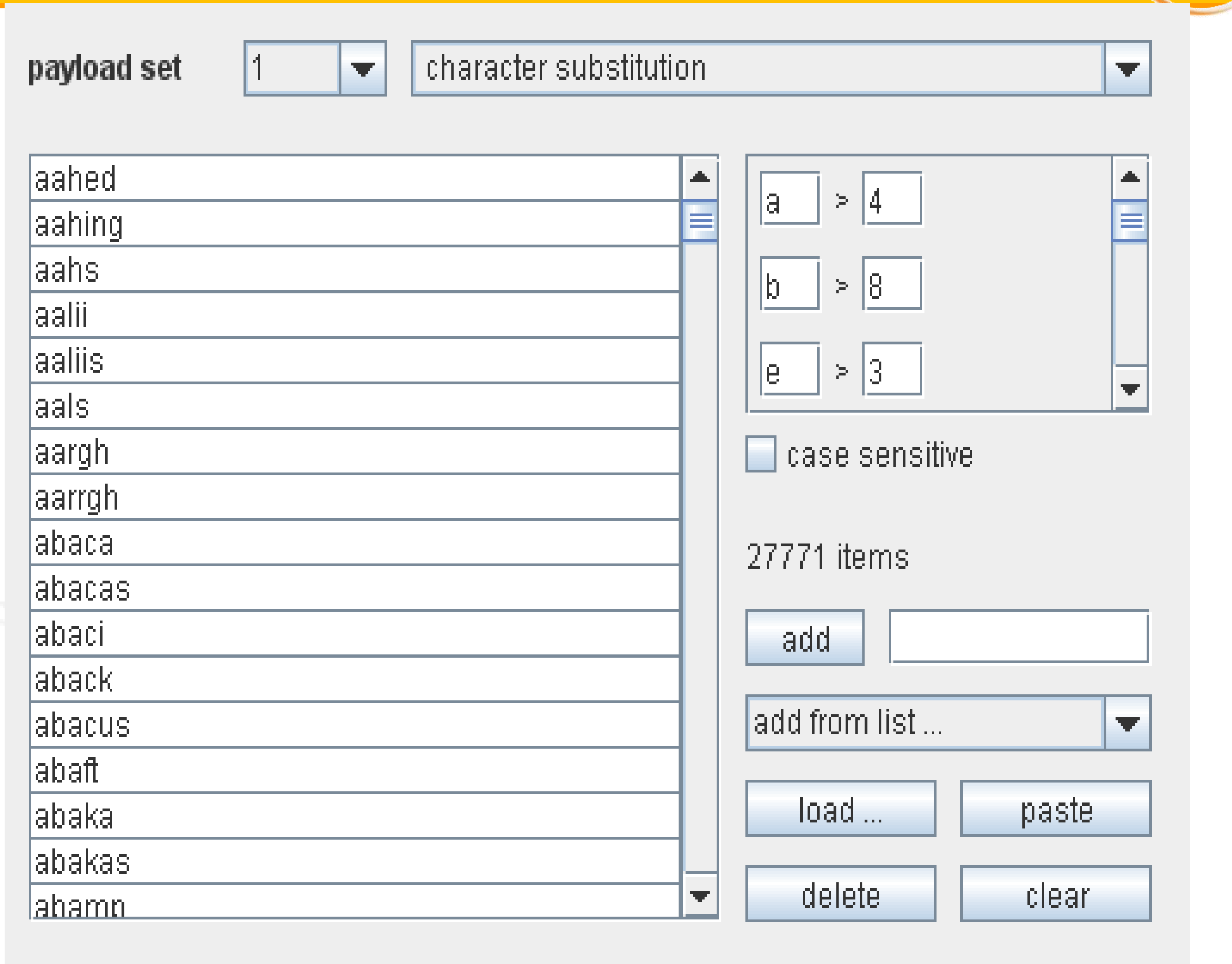
4.Enumerate domain lockout policy

5.Create a dictionary

6.Perform Attack

Brute force attack

- Brute force attack is a type of password guessing attack. In this type of attack, attackers systematically try every conceivable combination to find out the password of a user.



payload set 1 character substitution

aahed
aahing
aahs
aalii
aaliis
aals
aargh
aarrgh
abaca
abacas
abaci
aback
abacus
abaft
abaka
abakas
abamp

a > 4
b > 8
e > 3

□ case sensitive

27771 items

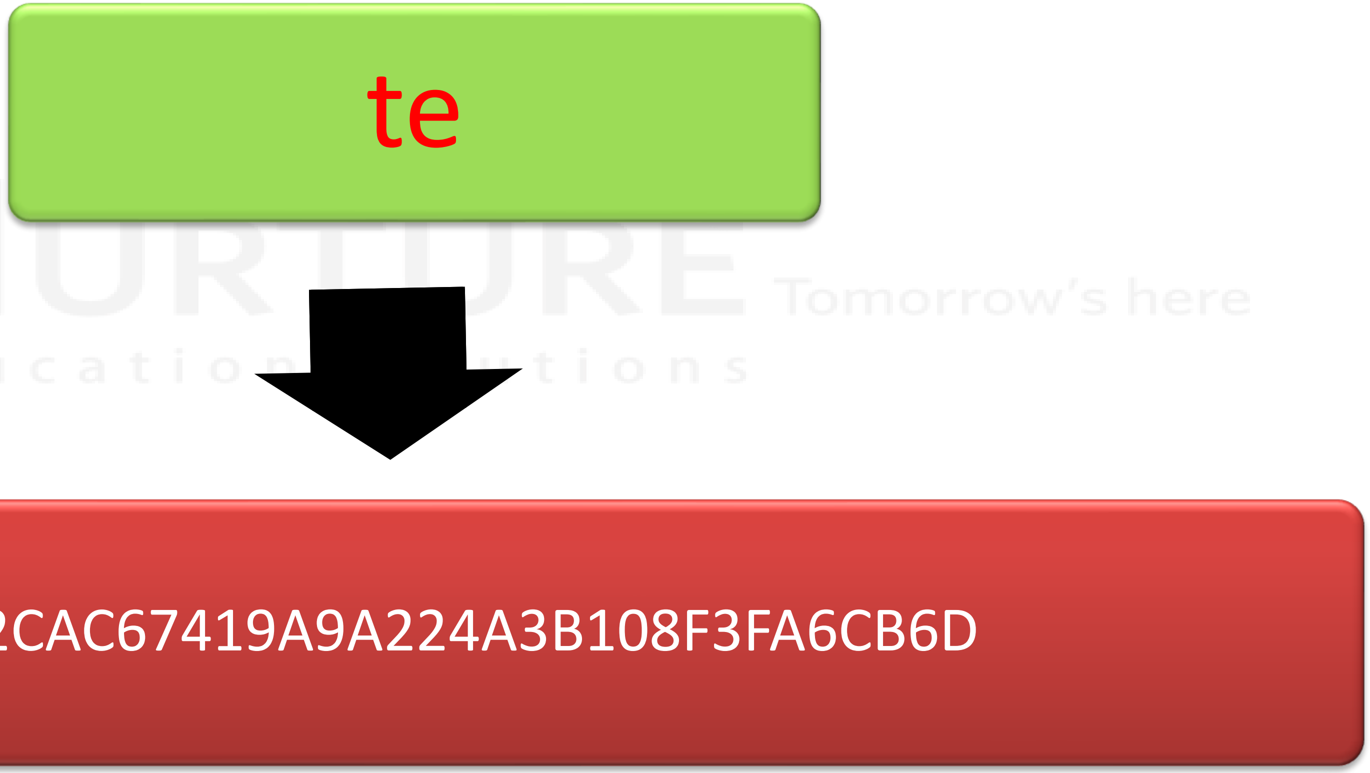
Password guessing program

Download link : http://portswigger.net/burp/help/intruder.html

How Windows Store Passwords

- LM “hashes”
  - Old technology used on LAN Manager
- NT hashes
  - Unicode password or MD4 hash
  - Used for authentication on more recent Windows systems

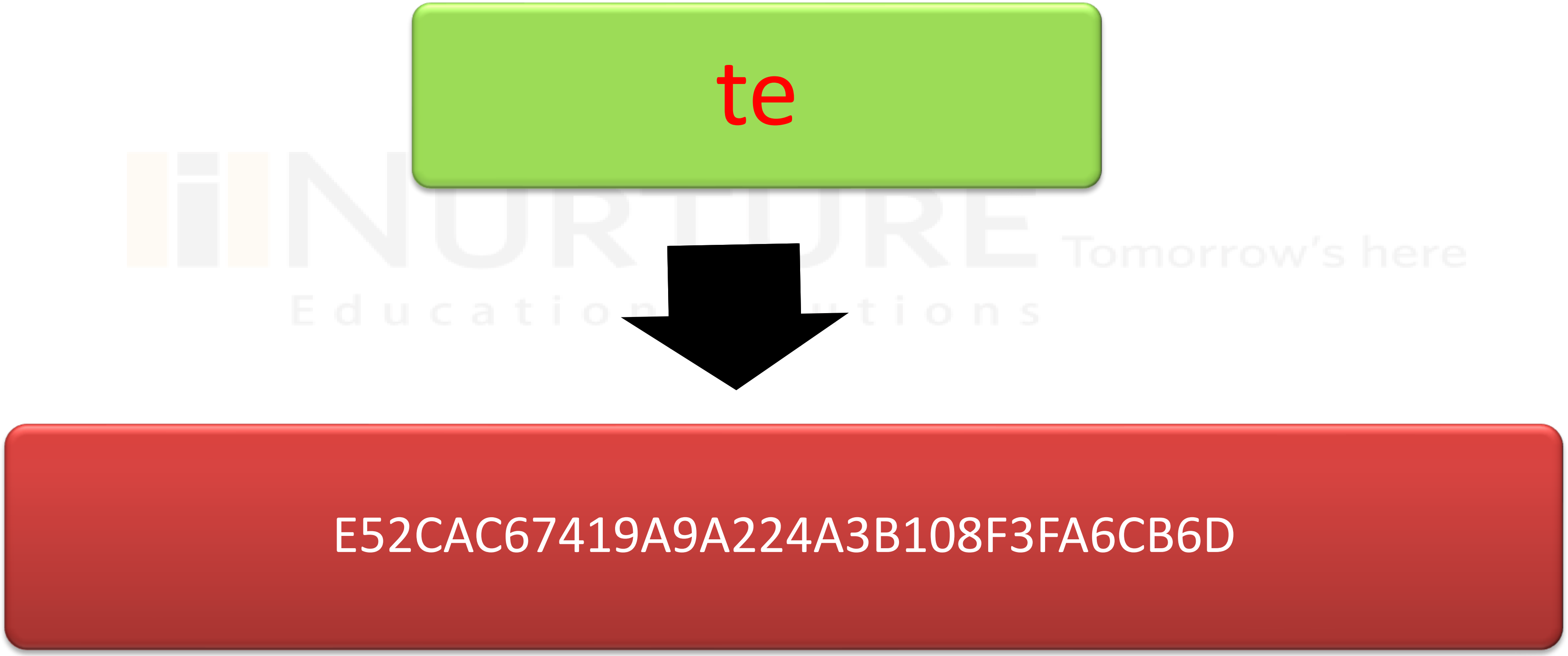
How a Hash looks Like



te

E52CAC67419A9A224A3B108F3FA6CB6D

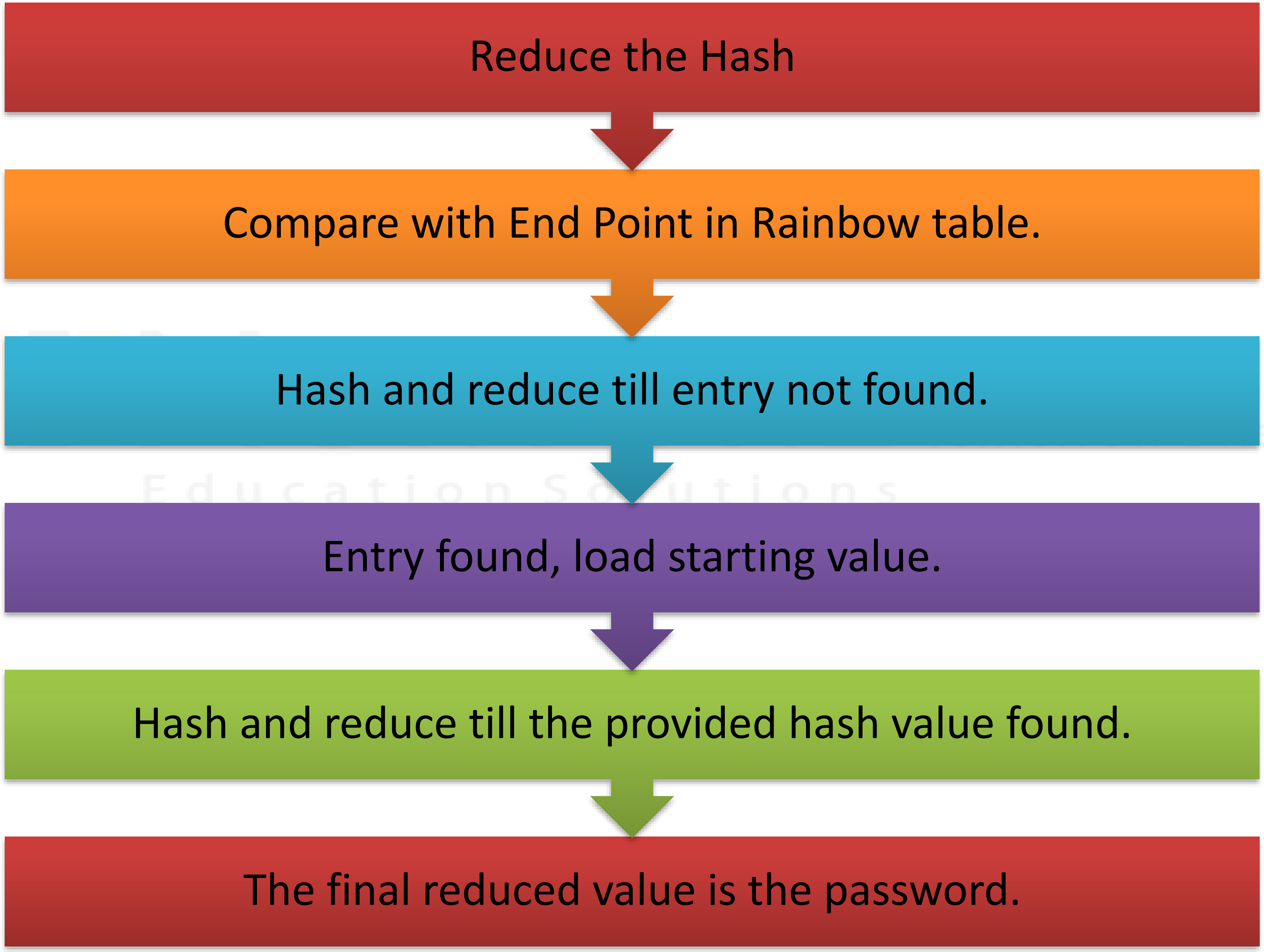
How a Hash looks Like



te

E52CAC67419A9A224A3B108F3FA6CB6D

Algorithm followed



Reduce the Hash

Compare with End Point in Rainbow table.

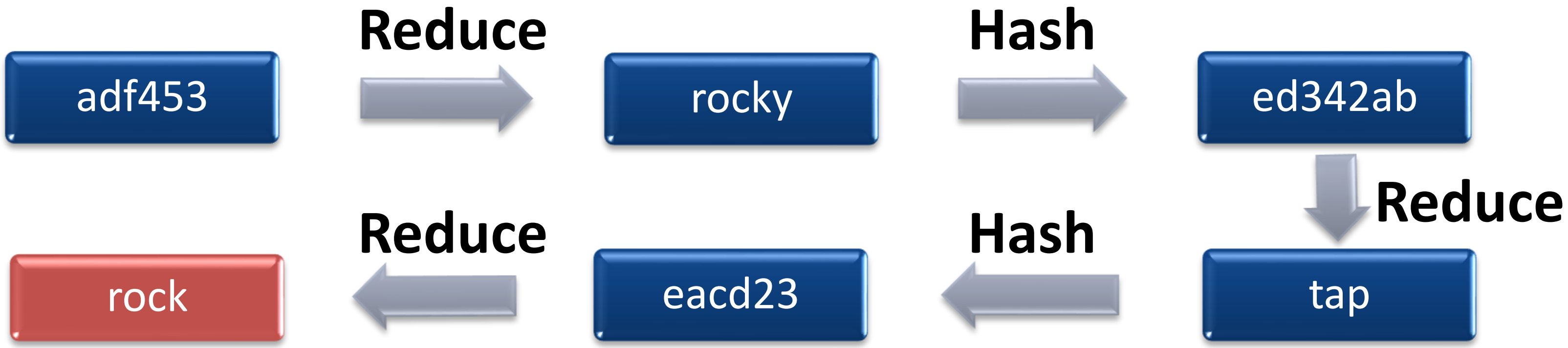
Hash and reduce till entry not found.

Entry found, load starting value.

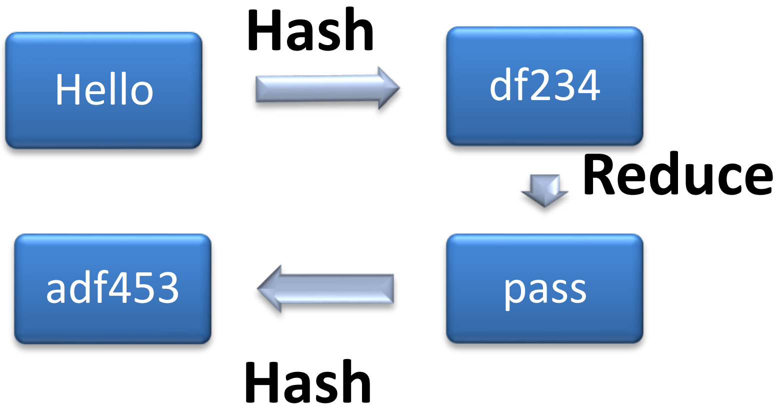
Hash and reduce till the provided hash value found.

The final reduced value is the password.

Process of Rainbow Table



adf453 → Reduce → rocky → Hash → ed342ab → Reduce → tap → Hash → eacd23 → Reduce → rock



Hello → Hash → df234 → Reduce → pass → Hash → adf453

START	END
joy	help
Hello	rock
Bottle	Mess
……….	………
passwd	linux23

Stochastic Forensics

Stochastic Forensics is a method to forensically reconstruct digital activity lacking artifacts, by analyzing emergent properties resulting from the stochastic nature of modern computers. Unlike traditional computer forensics, which relies on digital artifacts, stochastic forensics does not require artifacts and can therefore recreate activity which would otherwise be invisible. Its chief application is the investigation of insider data theft.

Stochastic : Having a random probability distribution or pattern that may be analyzed statistically but may not be predicted precisely.

Stochastic Forensics

- **Stochastic forensics** is a method to forensically reconstruct digital activity lacking artifacts, by analyzing emergent properties resulting from the stochastic nature of modern computers.

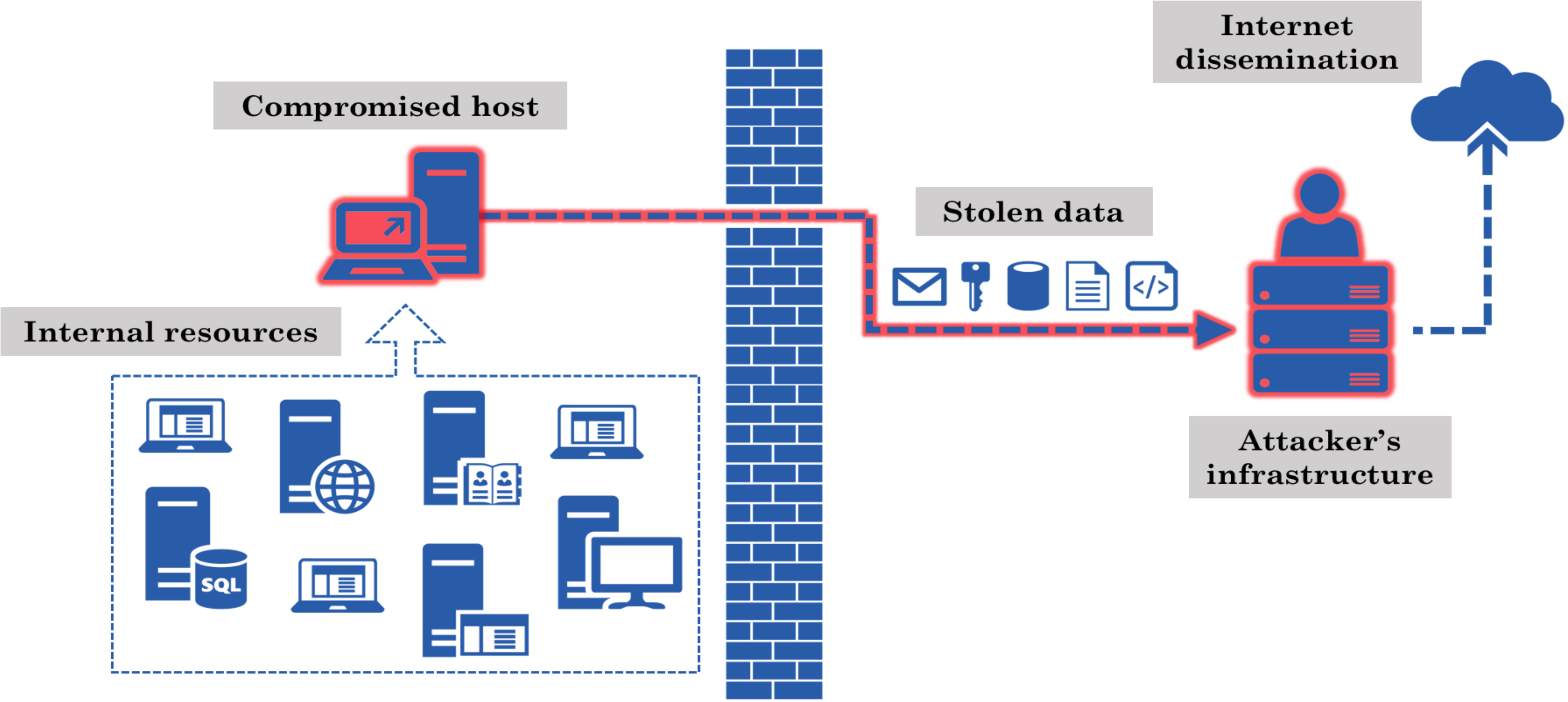
- Unlike traditional computer forensics, which relies on digital artifacts, stochastic forensics does not require artifacts and can therefore recreate activity which would otherwise be invisible.

Application

- Its chief application is the investigation of insider data theft

Why Stochastic Forensics?

Data Exfiltration



Stochastic Forensics

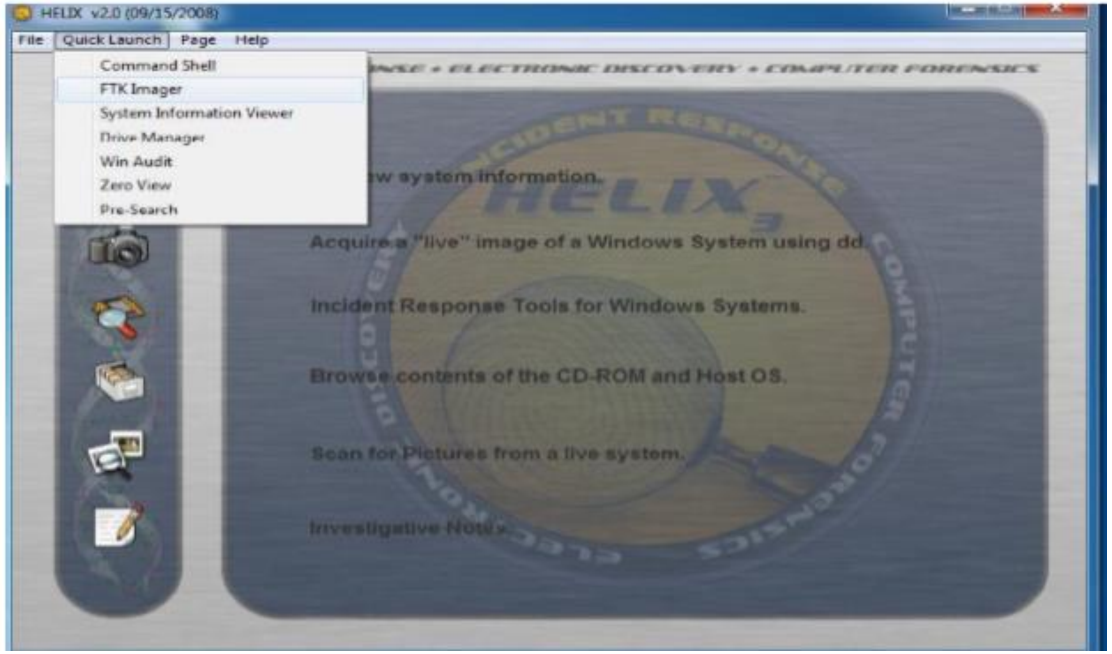
Stochastic forensics uses TIMESTAMP file is a data file created by ESRI mapping software, such as ArcMap or ArcCatalog.

It contains information about edits that have been made to a file geodatabase (. GDB file), which stores geographic information. TIMESTAMP files are not meant to be opened by the user.

Reference Material : https://www.slideshare.net/bluesme/catching-insider-data-theft-with-stochastic-forensics

Investigating Deleted Files Using Helix

- Kindly refer **practical with Helix R2009.1**
- Investigators use a variety of techniques and proprietary forensic applications to examine the **hard drive copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files**. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings.
- The **FTK imager of Helix Tool** is a powerful and flexible tool. It can be used to examine media and images and extracted deleted files.



...w system information.

Acquire a "live" image of a Windows System using dd.

Incident Response Tools for Windows Systems.

Browse contents of the CD-ROM and Host OS.

Scan for Pictures from a live system.

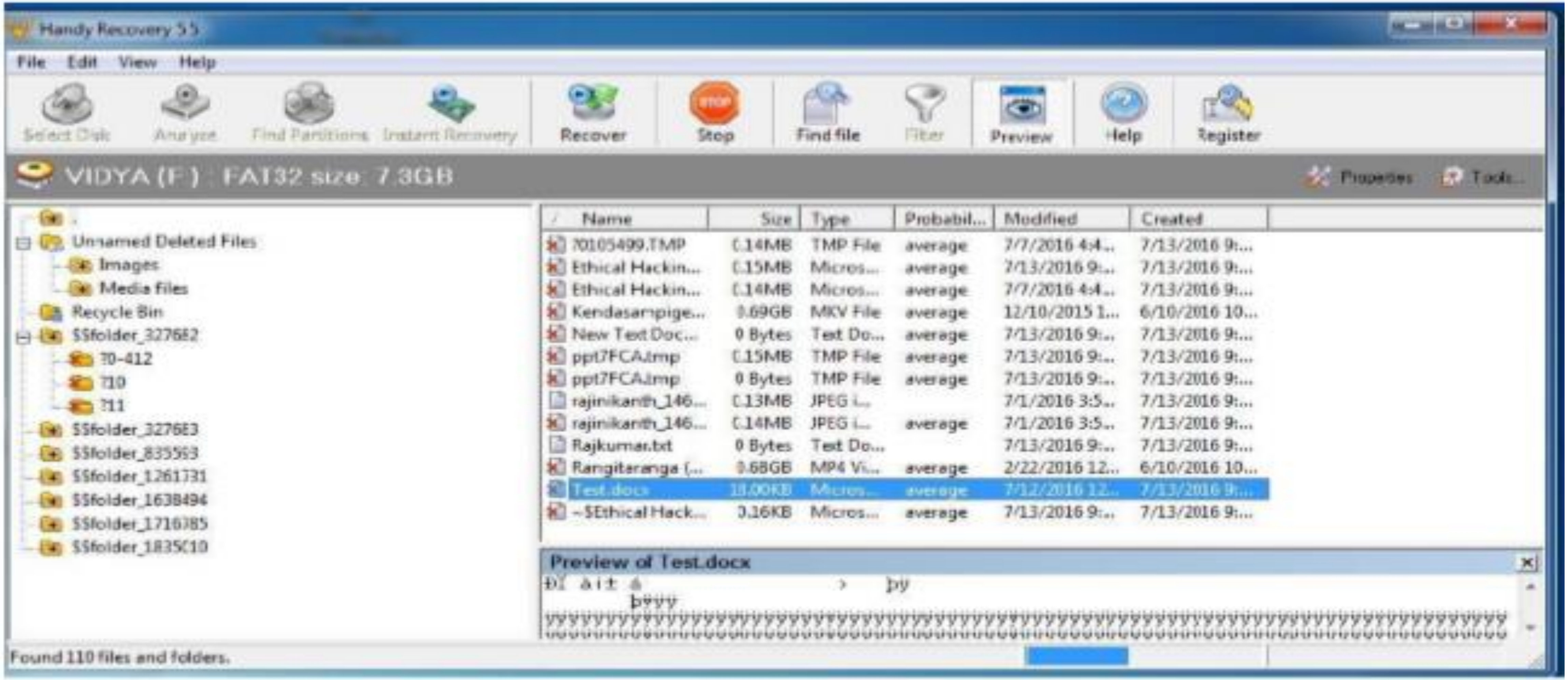
Investigative Notes.

The **Helix tool** is very **robust** and **free of charge**. Helix can be run as an **operating system;** it can be run from **command line,** and it also has a **windows GUI**. Helix allows for the analysis of a **live system**.

Reference Manual: https://apps.dtic.mil/dtic/tr/fulltext/u2/a585593.pdf

Investigating Deleted Files : Using Handy recovery tool

Kindly refer the practical for Used to recover deleted files from disk, previous lost partition from a disk.



- .
- Unnamed Deleted Files
  - Images
  - Media files
- Recycle Bin
- $$folder_327682
  - 70-412
  - 710
  - 711
- $$folder_327683
- $$folder_835563
- $$folder_1261731
- $$folder_1638494
- $$folder_1716385
- $$folder_1835010

Name	Size	Type	Probabil...	Modified	Created
70105499.TMP	0.14MB	TMP File	average	7/7/2016 4:4...	7/13/2016 9:...
Ethical Hackin...	0.15MB	Micros...	average	7/13/2016 9:...	7/13/2016 9:...
Ethical Hackin...	0.14MB	Micros...	average	7/7/2016 4:4...	7/13/2016 9:...
Kendasampige...	0.69GB	MKV File	average	12/10/2015 1...	6/10/2016 10...
New Text Doc...	0 Bytes	Text Do...	average	7/13/2016 9:...	7/13/2016 9:...
ppt7FCA.tmp	0.15MB	TMP File	average	7/13/2016 9:...	7/13/2016 9:...
ppt7FCA.tmp	0 Bytes	TMP File	average	7/13/2016 9:...	7/13/2016 9:...
rajinikanth_146...	0.13MB	JPEG i...		7/1/2016 3:5...	7/13/2016 9:...
rajinikanth_146...	0.14MB	JPEG i...	average	7/1/2016 3:5...	7/13/2016 9:...
Rajkumar.txt	0 Bytes	Text Do...		7/13/2016 9:...	7/13/2016 9:...
Rangitaranga (...	0.68GB	MP4 Vi...	average	2/22/2016 12...	6/10/2016 10...
Test.docx	18.00KB	Micros...	average	7/12/2016 12...	7/13/2016 9:...
~$Ethical Hack...	0.16KB	Micros...	average	7/13/2016 9:...	7/13/2016 9:...

Preview of Test.docx

Found 110 files and folders.

Email Investigations: Overview

- Click show original in an email
- Go to “***www.cyberforensics.in*** “and click ***Email Tracking***
- Go to who is website and gather information about intermediate nodes.
- If the message id is originating and is equal to the sender’s identity then the mail is not spoofed or else it is spoofed.

- Email has become a primary means of communication.
- Email can easily be forged.
- Email can be abused
  - Spam
  - Aid in committing a crime …
  - Threatening email, …

Email Investigations: Overview

- Email evidence:
    - Is in the email itself (header)
    - Left behind as the email travels from sender to recipient.
        - ✓ Contained in the various logs.
            - Law enforcement can use subpoenas
            - System ads have some logs.

Email Protocols: SMTP

- Neither IMAP or POP are involved relaying messages between servers.
- Simple Mail Transfer Protocol: SMTP
  - Easy, but can be spoofed easily.

Email Protocols: SMTP

```
From jholliday@engr.scu.edu Tue Dec 23 16:44:55 2003
Return-Path: <jholliday@engr.scu.edu>
Received: from server8.engr.scu.edu (root@server8.engr.scu.edu [129.210.16.8])
by server4.engr.scu.edu (8.12.10/8.12.10) with ESMTP id hBO0itpv008140
for <tschwarz@engr.scu.edu>; Tue, 23 Dec 2003 16:44:55 -0800
From: JoAnne Holliday <jholliday@engr.scu.edu>
Received: from 129.210.16.8 (dhcp-19-198.engr.scu.edu [129.210.19.198])
by server8.engr.scu.edu (8.12.10/8.12.10) with SMTP id hBO0W76P002752
for tschwarz; Tue, 23 Dec 2003 16:41:55 -0800 (PST)
Date: Tue, 23 Dec 2003 16:32:07 -0800 (PST)
Message-Id: <200312240041.hBO0W76P002752@server8.engr.scu.edu>
X-Spam-Checker-Version: SpamAssassin 2.60-rc3 (1.202-2003-08-29-exp) on
server4.engr.scu.edu
X-Spam-Level:
X-Spam-Status: No, hits=0.0 required=5.0 tests=none autolearn=ham version=2.60-r
c3
```

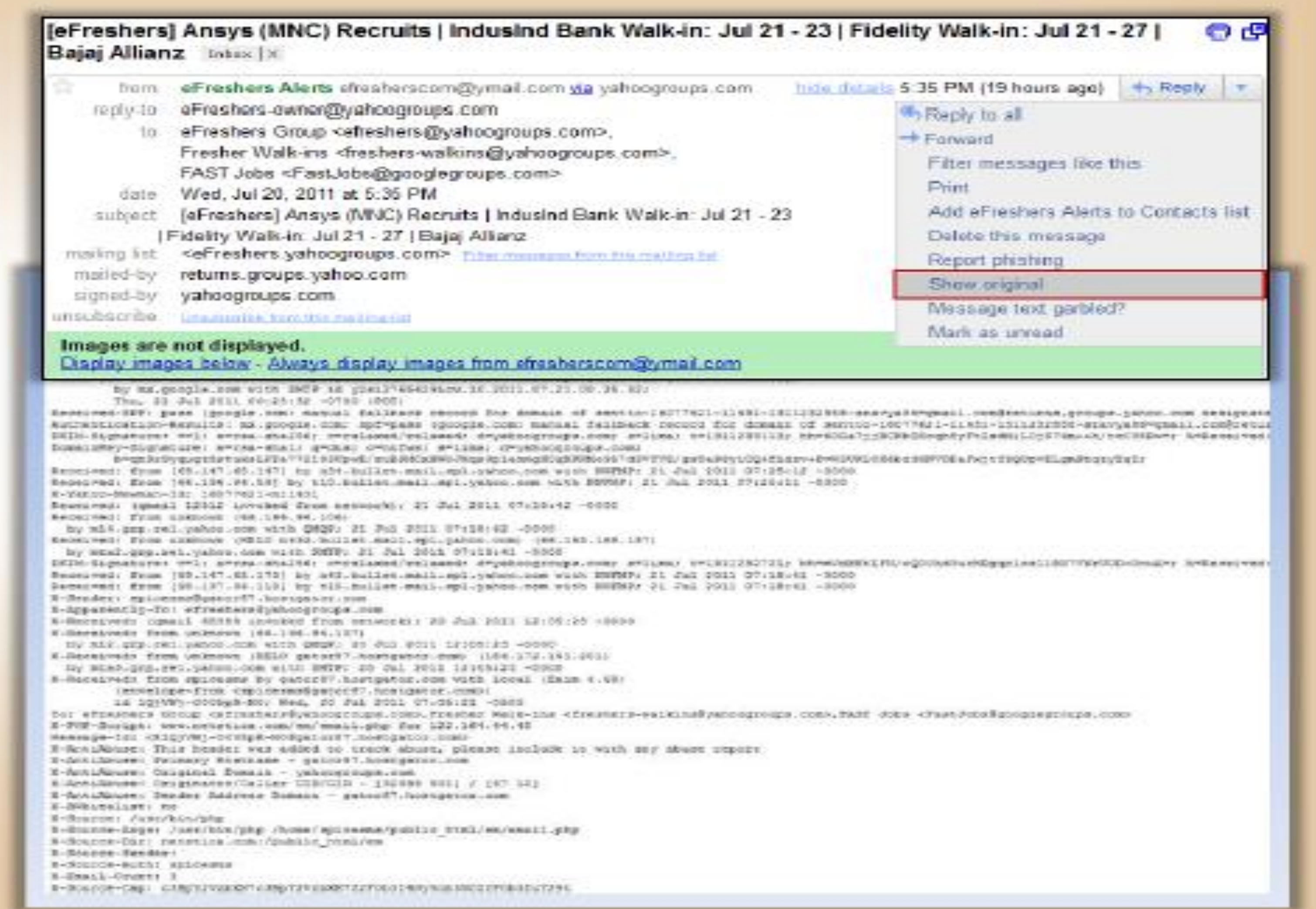
This looks very convincing.

Only hint: received line gives the name of my machine, defaulting to dhcp-19-198.

The DHCP server logs might tell you what machine this is, given the time. But you need to know the clock drift at the various machines.

Viewing Email Headers in Gmail

- Log on to Gmail and open the received email
- Click on the Reply drop-down button and navigate to the Show original option
- Select Message Headers - Full text and copy it
- Paste the text in any text editor and save the file
- Sign out of the Gmail account



[eFreshers] Ansys (MNC) Recruits | IndusInd Bank Walk-in: Jul 21 - 23 | Fidelity Walk-in: Jul 21 - 27 | Bajaj Allianz

from eFreshers Alerts efresherscom@ymail.com via yahoogroups.com

5:35 PM (19 hours ago)

reply-to eFreshers-owner@yahoogroups.com

to eFreshers Group <efreshers@yahoogroups.com>,
Fresher Walk-ins <freshers-walkins@yahoogroups.com>,
FAST Jobs <FastJobs@googlegroups.com>

date Wed, Jul 20, 2011 at 5:35 PM

subject [eFreshers] Ansys (MNC) Recruits | IndusInd Bank Walk-in: Jul 21 - 23 | Fidelity Walk-in: Jul 21 - 27 | Bajaj Allianz

mailing list <eFreshers.yahoogroups.com>

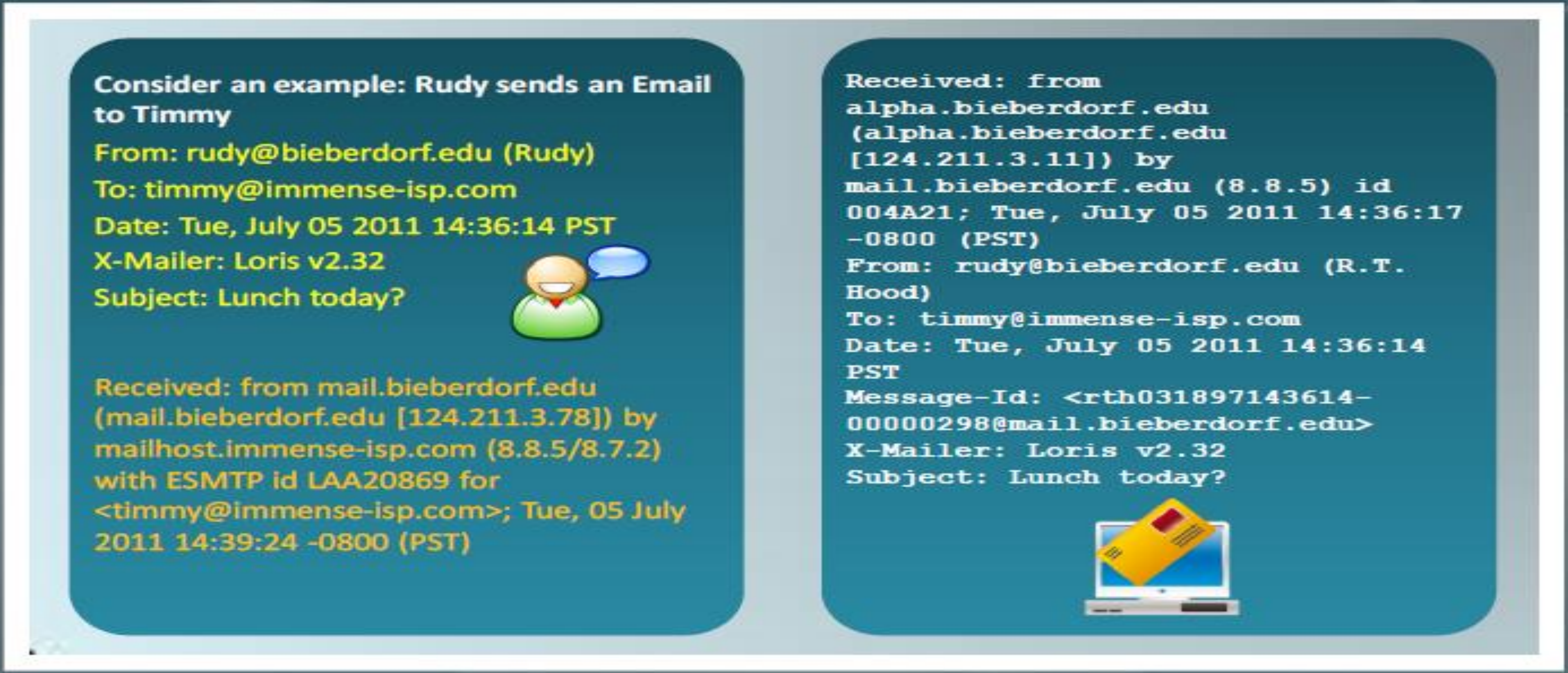
mailed-by returns.groups.yahoo.com

signed-by yahoogroups.com

unsubscribe

Images are not displayed.
Display images below - Always display images from efresherscom@ymail.com

[illegible]



Analyzing Email Headers

Consider an example: Rudy sends an Email to Timmy

From: rudy@bieberdorf.edu (Rudy)
To: timmy@immense-isp.com
Date: Tue, July 05 2011 14:36:14 PST
X-Mailer: Loris v2.32
Subject: Lunch today?

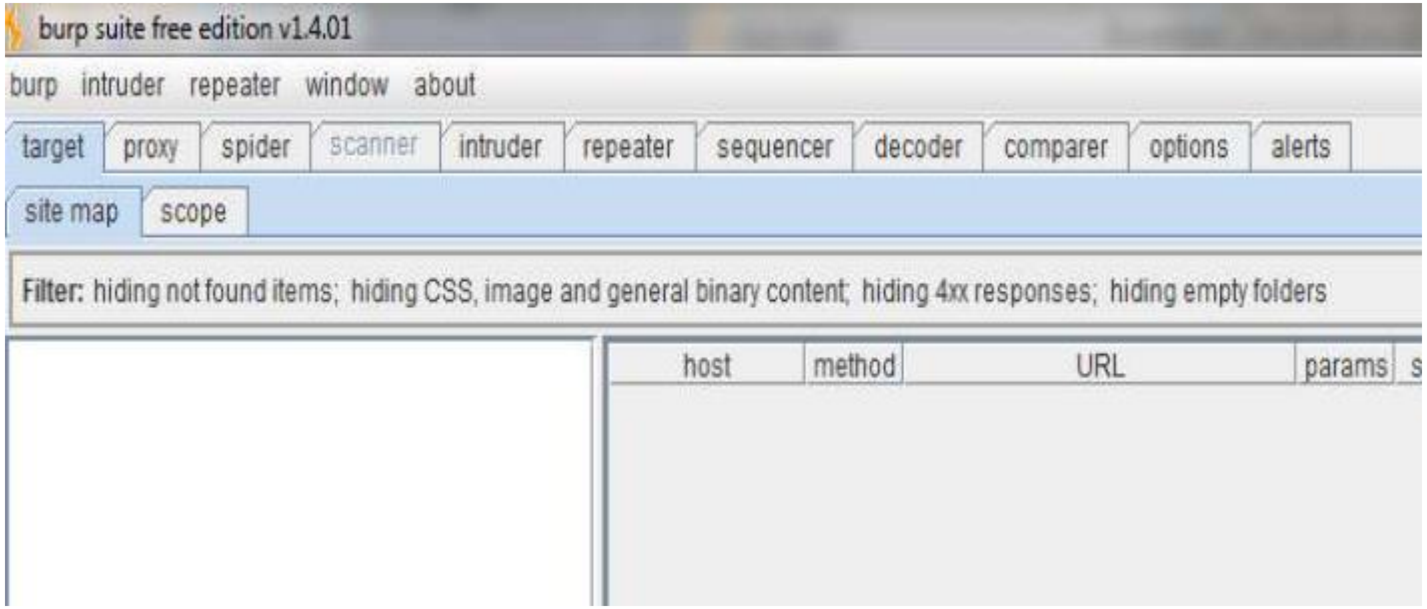
Received: from mail.bieberdorf.edu (mail.bieberdorf.edu [124.211.3.78]) by mailhost.immense-isp.com (8.8.5/8.7.2) with ESMTP id LAA20869 for <timmy@immense-isp.com>; Tue, 05 July 2011 14:39:24 -0800 (PST)

```
Received: from
alpha.bieberdorf.edu
(alpha.bieberdorf.edu
[124.211.3.11]) by
mail.bieberdorf.edu (8.8.5) id
004A21; Tue, July 05 2011 14:36:17
-0800 (PST)
From: rudy@bieberdorf.edu (R.T.
Hood)
To: timmy@immense-isp.com
Date: Tue, July 05 2011 14:36:14
PST
Message-Id: <rth031897143614-
00000298@mail.bieberdorf.edu>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Manual Testing of web application using Burp Suite

- *Burp Suite* is an integrated platform for performing security testing of web applications.

- It is designed to be used by hands-on testers to support the testing process. With a little bit of effort, anyone can start using the core features of *Burp* to test the security of their applications.



Filter: hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Using Burp Suite

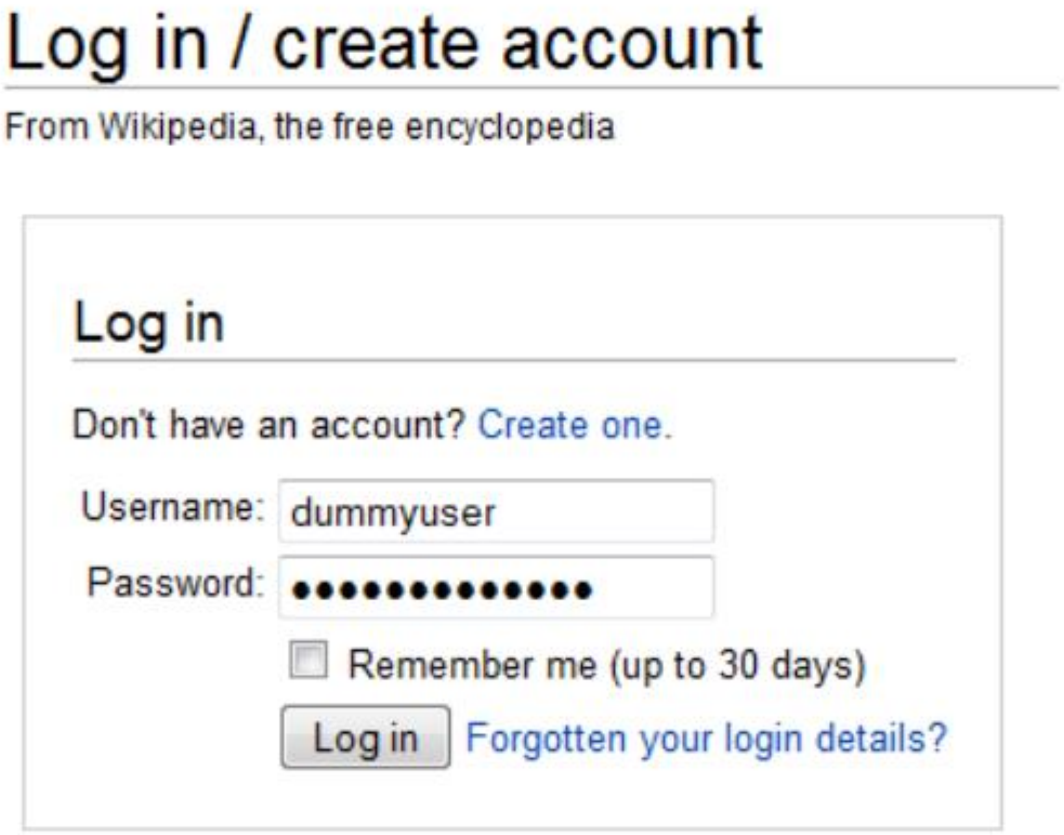
- ***Burp proxy***: Using ***Burp proxy***, one can intercept the traffic between the **browser** and **target application**.

- To demonstrate this feature, consider the following example of a Wikipedia login form (dummyuser: dummypassword) as shown in Figure.

- First, switch the **intercept mode "on"** in the suite.

- The **Forward option** allows you to send the packets from the source IP to the destination IP. The **Drop option** allows you to drop the packet if you feel it does not need analysis.

Using Burp Suite



Log in / create account

From Wikipedia, the free encyclopedia

Log in

Don't have an account? Create one.

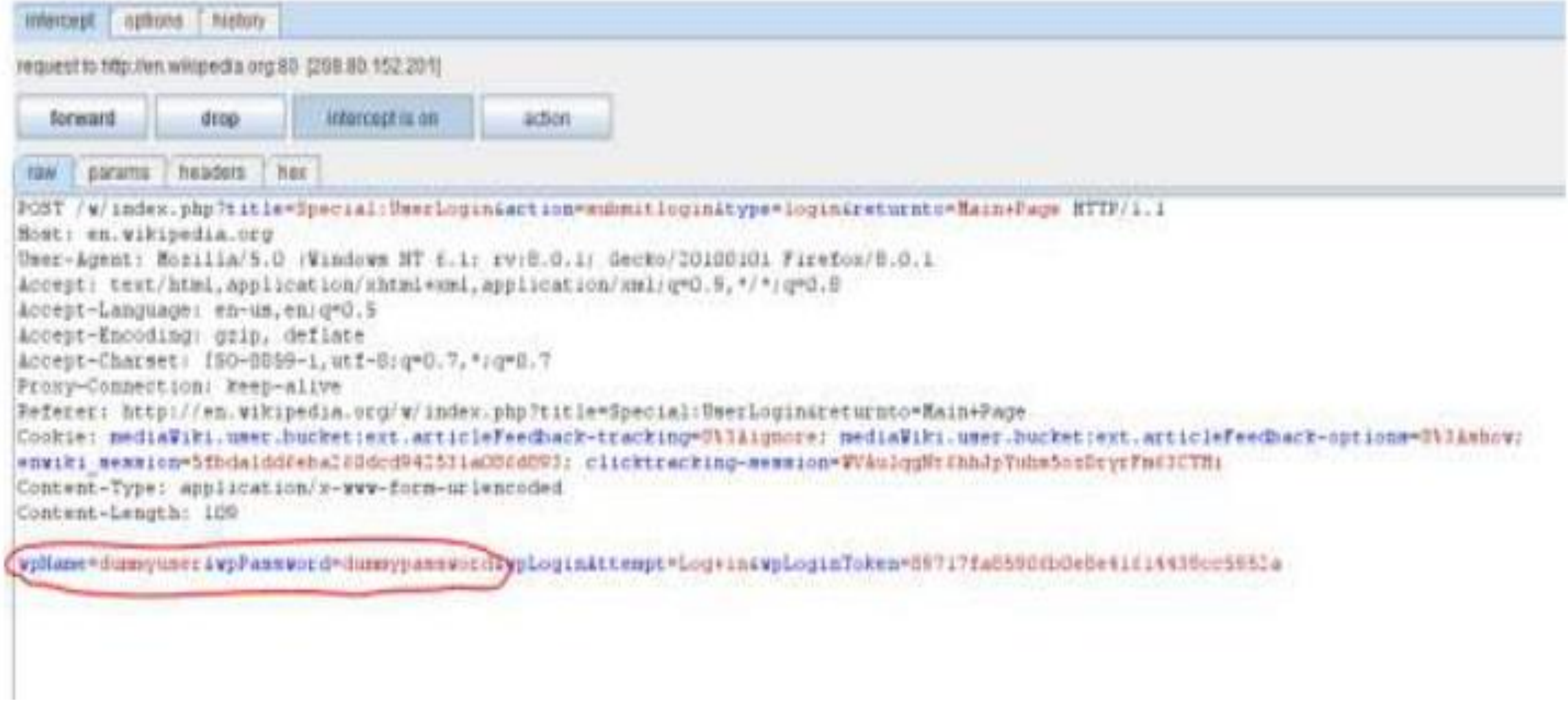
Username: dummyuser

Password: •••••••••••••

□ Remember me (up to 30 days)

Using Burp Suite

Below figure shows the login credentials of en.wikipedia.org being captured. Note that Wikipedia uses HTTP instead of HTTPS, hence the login credentials are captured in clear text.

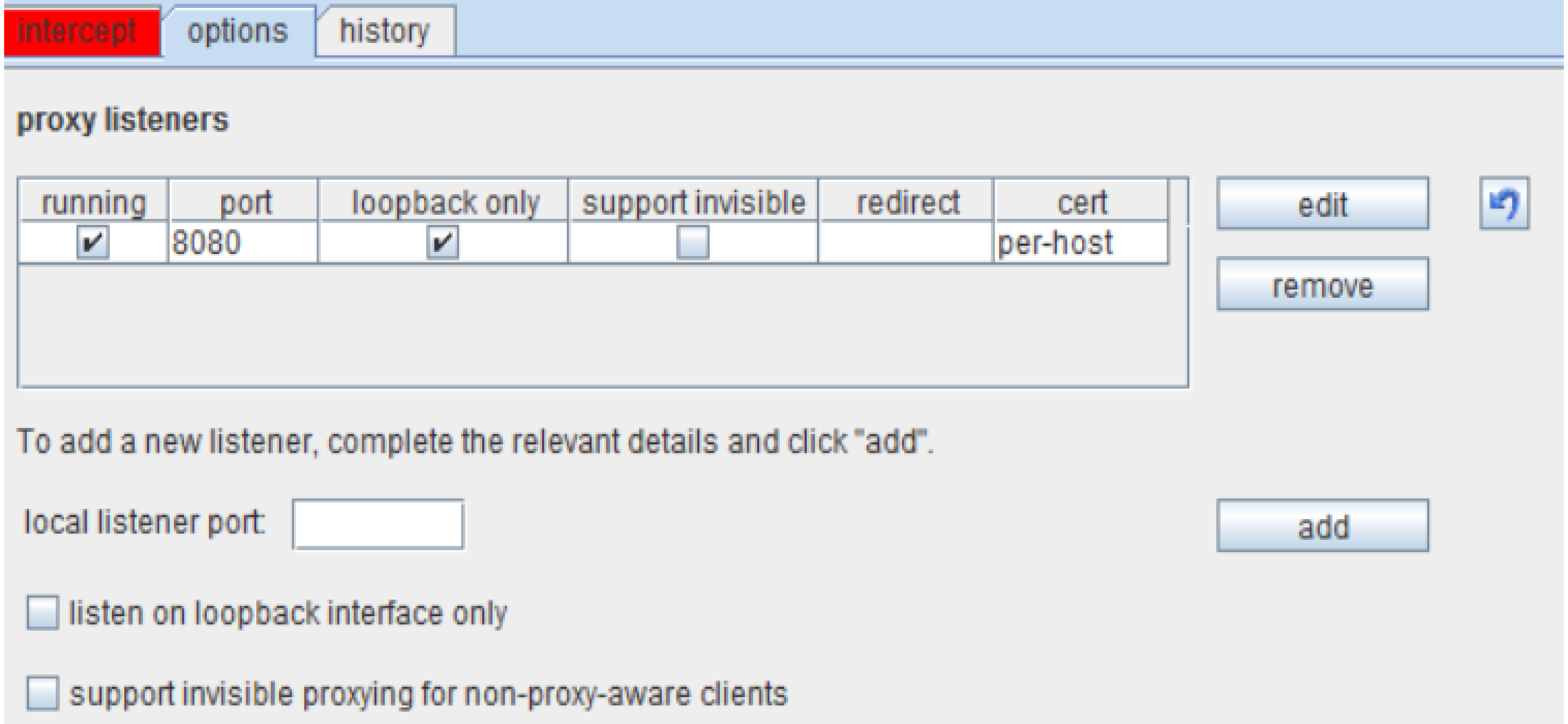


request to http://en.wikipedia.org:80 [208.80.152.201]

```
POST /w/index.php?title=Special:UserLogin&action=submitlogin&type=login&returnto=Main+Page HTTP/1.1
Host: en.wikipedia.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:8.0.1) Gecko/20100101 Firefox/8.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Proxy-Connection: keep-alive
Referer: http://en.wikipedia.org/w/index.php?title=Special:UserLogin&returnto=Main+Page
Cookie: mediaWiki.user.bucket:ext.articleFeedback-tracking=0%3Aignore; mediaWiki.user.bucket:ext.articleFeedback-options=0%3Ashow; enwiki_session=5fbda1dd6eba220dcd942531a006d093; clicktracking-session=WVAulqgNrfhhJpYubm5ozDryrFm6JCTM;
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

wpName=dummyuser&wpPassword=dummypassword&wpLoginAttempt=Log+in&wpLoginToken=88717fa8590db0e8e41f14430cc5852a
```

Using Burp Suite



proxy listeners

running	port	loopback only	support invisible	redirect	cert
☑	8080	☑	□		per-host

To add a new listener, complete the relevant details and click "add".

local listener port:

□ listen on loopback interface only

□ support invisible proxying for non-proxy-aware clients

Using Burp Suite

Intercepting messages

- The Intercept tab is used to display and modify HTTP and WebSocket messages that pass between your browser and web servers.

- The ability to monitor, intercept and modify all messages is a core part of Burp's user-driven workflow.

- In Burp Proxy's options, you can configure interception rules to determine exactly what HTTP requests and responses are stalled for interception (for example, in-scope items, items with specific file extensions, requests with parameters, etc.). You can also configure which WebSocket messages are intercepted.

Feel Free to ask for Any query

Ajay Shriram Kushwaha