

# TALLE DE ANÁLISIS DE LOGS

#fraternity



# Agenda

- **Módulo 1:** Introducción al análisis de log
- **Módulo 2:** Extracción, parseo y normalización
- **Módulo 3:** Preparación del laboratorio
  - (Almuerzo)
- **Módulo 4:** Análisis con ELK
- **Módulo 5:** Práctica de análisis

# Carga de los datos

***<https://bit.ly/2yQc7XZ>***



# MÓDULO 1: *INTRODUCCIÓN AL ANÁLISIS DE LOGS*

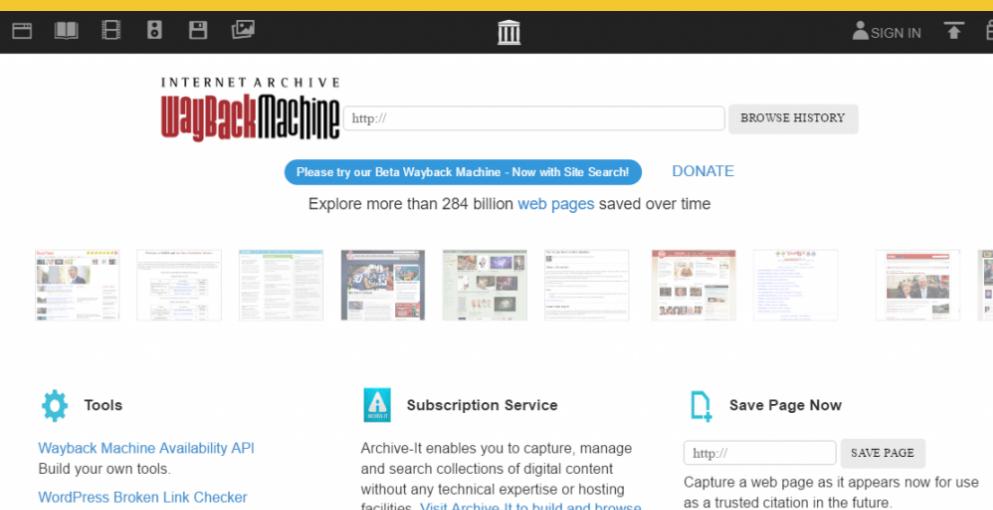
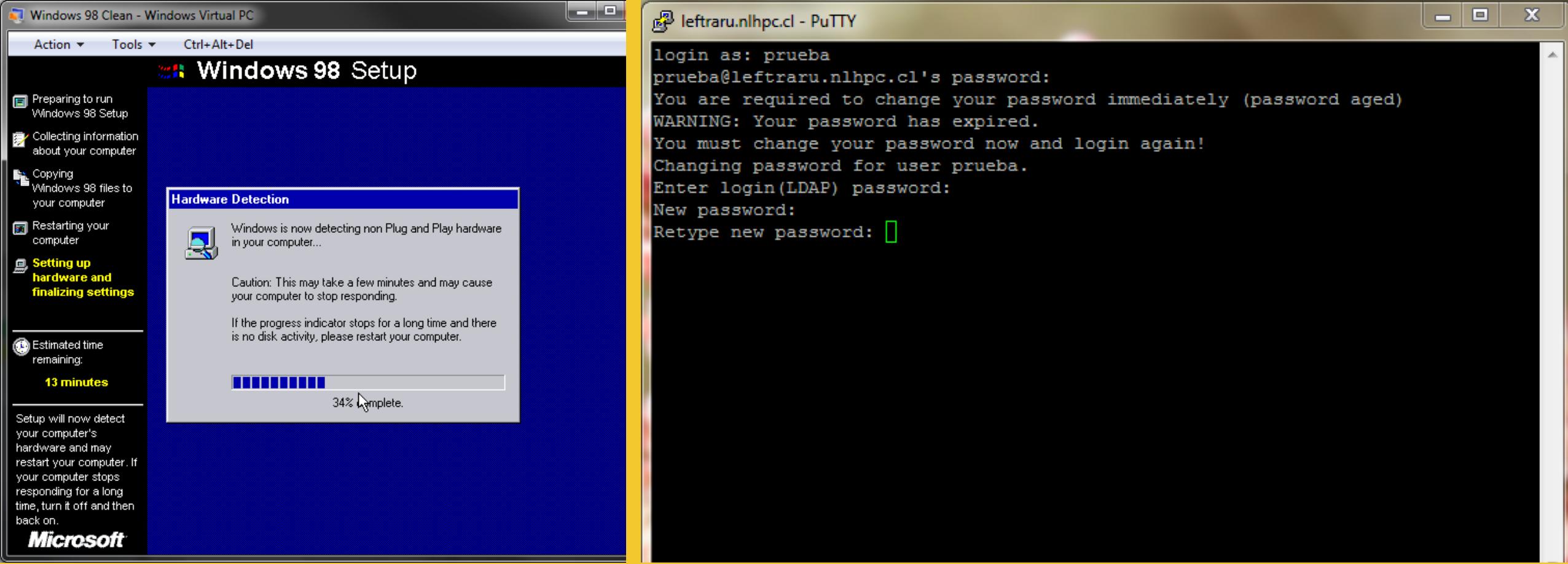
# Estructura del Módulo 1

- ¿Qué son los logs?
- ¿Cómo son los logs?
- ¿Por qué son importantes?
- Conceptos claves

# ¿Qué c#%ch@ es un log?

- El registro de un evento que ocurrió en algún sistema que procesa información.
  - *Información relevante.*
  - *En un momento determinado.*
  - *En un contexto.*
  - *Con una acción.*
  - *Quien la hizo.*





TODO DEJA UN RASTRO...  
UN REGISTRO



¿CÓMO SON  
LOS LOGS?

```
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: logInterfaces File: ../../vpn/AgentUtilities/Routing/InterfaceRouteMonitorCommon.cpp Line: 477 IP Address Interface List: FE80:0:0:0:384D:BDFF:FE57:6715 FE80:0:0:0:5F5B:CD0D:F800:DB4E FE80:0:0:0:5AFD:A6DE:D8E3:BD5E FE80:0:0:0:AEDE:48FF:FE00:1122
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: netInterfaceNoticeCategoryHandler File: ../../vpn/Agent/MainThread.cpp Line: 7794 Network Interface change detected, refreshing physical MAC addresses
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun0". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun1". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun0". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun1". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: GetPrimaryInterfaceIndex File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 422 Unable to get global IPv4 information from system configuration.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun0". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun1". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: determinePublicAddrCandidateFromDefRoute File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 1825 Invoked Function: CHostConfigMgr::FindDefaultRouteInterface Return Code: -24117215 (0xFE900021) Description: ROUTETABLE_ERROR_GETBESTROUTE_FAILED
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: updatePotentialPublicAddresses File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 1956 Invoked Function: CHostConfigMgr::determinePublicAddrCandidateFromDefRoute Return Code: -24117215 (0xFE900021) Description: ROUTETABLE_ERROR_GETBESTROUTE_FAILED
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: GetPrimaryInterfaceIndex File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 422 Unable to get global IPv6 information from system configuration.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: updatePotentialPublicAddresses File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 1970 Invoked Function: CHostConfigMgr::determinePublicAddrCandidateFromDefRoute Return Code: -28835823 (0xFE480011) Description: HOSTCONFIGMGR_ERROR_SUPPORTED_PUBLIC_ADDRESS_UNAVAILABLE
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: DeterminePublicInterface File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 2356 Invoked Function: CHostConfigMgr::updatePotentialPublicAddresses Return Code: -28835824 (0xFE480010) Description: HOSTCONFIGMGR_ERROR_PUBLIC_ADDRESS_UNAVAILABLE
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: applyHostConfigForNoVpn File: ../../vpn/Agent/MainThread.cpp Line: 10375 Invoked Function: CHostConfigMgr::DeterminePublicInterface Return Code: -28835824 (0xFE480010) Description: HOSTCONFIGMGR_ERROR_PUBLIC_ADDRESS_UNAVAILABLE
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: OnTimerExpired File: ../../vpn/Agent/MainThread.cpp Line: 5825 Invoked Function: CMainThread::applyHostConfigForNoVpn Return Code: -28835824 (0xFE480010) Description: HOSTCONFIGMGR_ERROR_PUBLIC_ADDRESS_UNAVAILABLE
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: GetPrimaryInterfaceIndex File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 422 Unable to get global IPv4 information from system configuration.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: determinePublicAddrCandidateFromDefRoute File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 1825 Invoked Function: CHostConfigMgr::FindDefaultRouteInterface Return Code: -24117215 (0xFE900021) Description: ROUTETABLE_ERROR_GETBESTROUTE_FAILED
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: updatePotentialPublicAddresses File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 1956 Invoked Function: CHostConfigMgr::determinePublicAddrCandidateFromDefRoute Return Code: -24117215 (0xFE900021) Description: ROUTETABLE_ERROR_GETBESTROUTE_FAILED
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: GetPrimaryInterfaceIndex File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 422 Unable to get global IPv6 information from system configuration.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: updatePotentialPublicAddresses File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 1970 Invoked Function: CHostConfigMgr::determinePublicAddrCandidateFromDefRoute Return Code: -28835823 (0xFE480011) Description: HOSTCONFIGMGR_ERROR_SUPPORTED_PUBLIC_ADDRESS_UNAVAILABLE
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: DeterminePublicInterface File: ../../vpn/AgentUtilities/HostConfigMgr.cpp Line: 2356 Invoked Function: CHostConfigMgr::updatePotentialPublicAddresses Return Code: -28835824 (0xFE480010) Description: HOSTCONFIGMGR_ERROR_PUBLIC_ADDRESS_UNAVAILABLE
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: OnTimerExpired File: ../../vpn/Agent/MainThread.cpp Line: 5850 Invoked Function: CHostConfigMgr::DeterminePublicInterface Return Code: -28835824 (0xFE480010) Description: HOSTCONFIGMGR_ERROR_PUBLIC_ADDRESS_UNAVAILABLE
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun0". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:29 NT-SYSTEM acvpnagent[50]: Function: getInterfacesInternal File: ../../vpn/Common/Utility/NetInterface_unix.cpp Line: 1396 missing PPP destination address for interface "utun1". Check profile PPPExclusion (set to Automatic?) or contact your administrator.
Oct 19 08:23:30 NT-SYSTEM BetterTouchTool[29798]: assertion failed: 17G65: libxpc.dylib + 75013 [0BC7AD67-671D-31D4-8B88-C317B8379598]: 0x89
Oct 19 08:23:30 NT-SYSTEM systemstats[54]: assertion failed: 17G65: systemstats + 914800 [D1E75C38-62CE-3D77-9ED3-5F6D38EF0676]: 0x40
```

# Un log de NGINX

(/var/log/nginx/access.log)

```
66.249.65.159 - - [06/Nov/2014:19:10:38 +0600] "GET /news/53f8d72920ba2744fe873ebc.html  
HTTP/1.1" 404 177 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26  
(KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1;  
+http://www.google.com/bot.html)"  
  
66.249.65.3 - - [06/Nov/2014:19:11:24 +0600] "GET  
/?q=%E0%A6%AB%E0%A6%BE%E0%A7%9F%E0%A6%BE%E0%A6%B0 HTTP/1.1" 200 4223 "-" "Mozilla/5.0  
(compatible; Googlebot/2.1; +http://www.google.com/bot.html)"  
  
66.249.65.62 - - [06/Nov/2014:19:12:14 +0600] "GET  
/?q=%E0%A6%A6%E0%A7%8B%E0%A7%9F%E0%A6%BE HTTP/1.1" 200 4356 "-" "Mozilla/5.0 (compatible;  
Googlebot/2.1; +http://www.google.com/bot.html)"
```

# El detalle...

```
66.249.65.159 -- [06/Nov/2014:19:10:38 +0600] "GET /news/53f8d72920ba2744fe873ebc.html  
HTTP/1.1" 404 177 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26  
(KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1;  
+http://www.google.com/bot.html)"
```

- 66.249.65.159
- -
- 06/Nov/2014:19:10:38 **+0600**
- GET
- /news/53f8d72920ba2744fe873ebc.html
- HTTP/1.1
- 404
- 177
- "-"
- Mozilla/5.0 (iPhone; CPU iPhone OS 6\_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko)<sup>nginx</sup>  
Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1;  
+http://www.google.com/bot.html)

# ¿Cómo se estructura?

log\_format combined:

```
'$remote_addr - $remote_user [$time_local] ' "$request" $status $body_bytes_sent'  
'"$http_referer" "$http_user_agent";'
```

[http://nginx.org/en/docs/http/ngx\\_http\\_log\\_module.html](http://nginx.org/en/docs/http/ngx_http_log_module.html)

# Pero la vida... no siempre sonríe ☹

```
1 DNS Server log file creation at 1/22/2018 4:57:21 PM
2
3 Message logging key (for packets - other items use a subset of these fields):
4 Field # Information      Values
5 -----
6   1 Date
7   2 Time
8   3 Thread ID
9   4 Context
10  5 Internal packet identifier
11  6 UDP/TCP indicator
12  7 Send/Receive indicator
13  8 Remote IP
14  9 Xid (hex)
15  10 Query/Response      R = Response
16          | blank = Query
17  11 Opcode              Q = Standard Query
18          | N = Notify
19          | U = Update
20          | ? = Unknown
21  12 [ Flags (hex)
22  13 Flags (char codes) A = Authoritative Answer
23          | T = Truncated Response
24          | D = Recursion Desired
25          | R = Recursion Available
26  14 ResponseCode ]
27  15 Question Type
28  16 Question Name
29
30 1/22/2018 4:57:22 PM 1394 PACKET 000000CE5B16D8C0 UDP Rcv 127.0.0.1      bed7  Q [0001  D  NOERROR] CNAME  (36)ef2a673f-6ec4-42a8-a8bd-8f824394e2f4(6)
31
32 1/22/2018 4:57:22 PM 1394 PACKET 000000CE5B16D8C0 UDP Snd 127.0.0.1      bed7 R Q [8085 A DR  NOERROR] CNAME  (36)ef2a673f-6ec4-42a8-a8bd-8f824394e2f4(6)
33
34 1/22/2018 4:57:37 PM 1394 PACKET 000000CE5B16F840 UDP Rcv 127.0.0.1      bd66  Q [0001  D  NOERROR] A       (10)vortex-win(4)data(9)microsoft(3)com(0)
35
```

Logs DNS Windows Server

Y se puede  
poner  
peor...

Log de  
Windows...

Event 4663, Microsoft Windows security auditing.

General Details

Friendly View  XML View

```
- <Event
  xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  + <System>
  - <EventData>
    <Data Name="SubjectUserId" value="S-1-5-21-1074975393-3132328237-1375513134-1104"/>
    <Data Name="SubjectUserName" value="test001"/>
    <Data Name="SubjectDomainName" value="CONTOSO"/>
    <Data Name="SubjectLogonId" value="0x464873"/>
    <Data Name="ObjectServer" value="Security"/>
    <Data Name="ObjectType" value="File"/>
    <Data Name="ObjectName" value="C:\Files\Test007.txt"/>
    <Data Name="HandleId" value="0xfc"/>
    <Data Name="AccessList" value="%%4417"/>
    <Data Name="AccessMask" value="0x2"/>
    <Data Name="ProcessId" value="0xacc"/>
    <Data Name="ProcessName" value="C:\Windows\System32\notepad.exe"/>
  </EventData>
</Event>
```

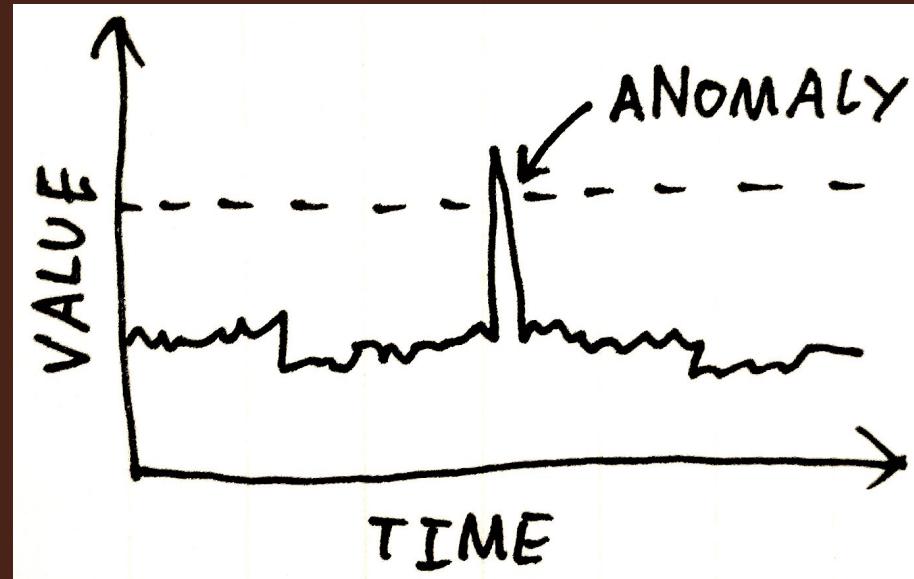
# Y aun peor...

```
Exception in thread "main" java.lang.IllegalStateException: A book has a null property
    at com.example.myproject.Author.getBookIds(Author.java:38)
    at com.example.myproject.Bootstrap.main(Bootstrap.java:14)
Caused by: java.weblayer.ZzzException
    at com.example.weblayer.Book.getId(WebBook.java:12)
    at com.example.weblayer.Author.getBookIds(WebAuthor.java:38)
Caused by: java.servicelayer.YyyException
    at com.example.servicelayer.Book.getId(BookService.java:220)
    at com.example.servicelayer.Author.getBookIds(AuthorService.java:350)
Caused by: java.componentlayer.NullPointerException
    at com.example.componentlayer.Book.getId(Book.java:22)
    at com.example.componentlayer.Author.getBookIds(Author.java:35)
Caused by: java.lang.daolayer.XxxException
    at com.example.daolayer.Book.getId(BookDao.java:22)
    at com.example.daolayer.Author.getBookIds(AuthorDao.java:35)
    ... 1 more
```

**Root Cause may  
in the middle**

# Parseadores y scripting al rescate!





¿POR QUÉ SON  
IMPORTANTES?

# Puntos importantes desde un punto de seguridad

- Las máquinas son buenas detectando firmas, no comportamientos de forma automágica.
- Siempre, siempre, han dado algo de que hablar.
- Dicen todo lo que pasó... *lo que esperamos y lo que no, lo bueno y lo malo.*
- *Cuando hay que explicar algo, es la única forma de hacerlo.*

**“Ojos que no ven... sistema que  
hackean...”**

# Buscando anomalías...



# User Agents...

User Agent	Count
DirBuster-0.12 ( <a href="http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project">http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project</a> )	1,289,186
-	71,237
Nessus	573
/*	345
w3af.sourceforge.net	107
Nessus SOAP v0.0.1 (Nessus.org)	91
webmin	84
"; system(id);#	81
NESSUS::SOAP	79
mercuryboard_user_agent_sql_injection.nasl'	77

# Métodos...

Method	Count
HEAD	1,290,225
POST	36,363
GET	33,456
-	848
OPTIONS	296
CONNECT	241
DELETE	211
GNUTELLA	168
SEARCH	121
PUT	116



# CONCEPTOS IMPORTANTES

# Conceptos Clave

- Timestamp (Time-Zone)
- Contexto
- Campos clave
- Indicadores de Compromiso
- TTP (Tácticas, Herramientas y Procedimientos)
- Correlación de Logs
- Kill-Chain
- Procesamiento de Logs (*Módulo 2*)

# Timestamp / Time Zone

El momento en que un determinado evento ocurrió...

Sin embargo:

- ¿Está bien la hora del servidor que registró el evento?
- Estructura de Hora (YYYY-dd-MM HH:mm:ssTZ)
- Unix Epoch (1 de Enero, 1970) - Lo ideal
- GMT-0 / UTC es lo mismo
- Jamás perder de vista este aspecto!!

<https://www.epochconverter.com/>

# Saber cuál es el contexto...

Entender el contexto del o que se está analizando **es CLAVE**.

Si no se comprende correctamente, lo que estamos viendo nos llevará a realizar análisis engañosos.



# Campos Claves

Saber lo que se está buscando permitirá saber qué información es útil para la búsqueda, y cual no.

Diseñar un análisis requiere preparación y saber que pregunta se busca responder.

Los campos claves permiten obtener las respuestas que buscamos...

Knowing  
what you want  
is  
the first step  
toward  
getting it.

--Mae West



# Indicadores de Compromiso

- Los indicadores de compromiso permiten buscar en los **campos claves** indicadores de que efectivamente existió un ataque o hay uno en progreso.
- Son las huellas evidentes de que algo malo ocurrió.
- Ejemplos:
  - *Hashes*
  - *Direcciones IP (origenes)*
  - *Puertos*
  - *URL's*
  - *Correos*
  - *Etcétera...*

# TTP (Tácticas, Herramientas y Procedimientos)

Son los comportamientos, patrones o indicadores de ataque que permiten entender a mayor cabalidad que existe un ataque en progreso.

- **Tácticas:** ¿Qué es lo que hacen?
- **Herramientas:** ¿Qué herramientas utilizan?
- **Procedimientos:** ¿Cómo lo hacen?



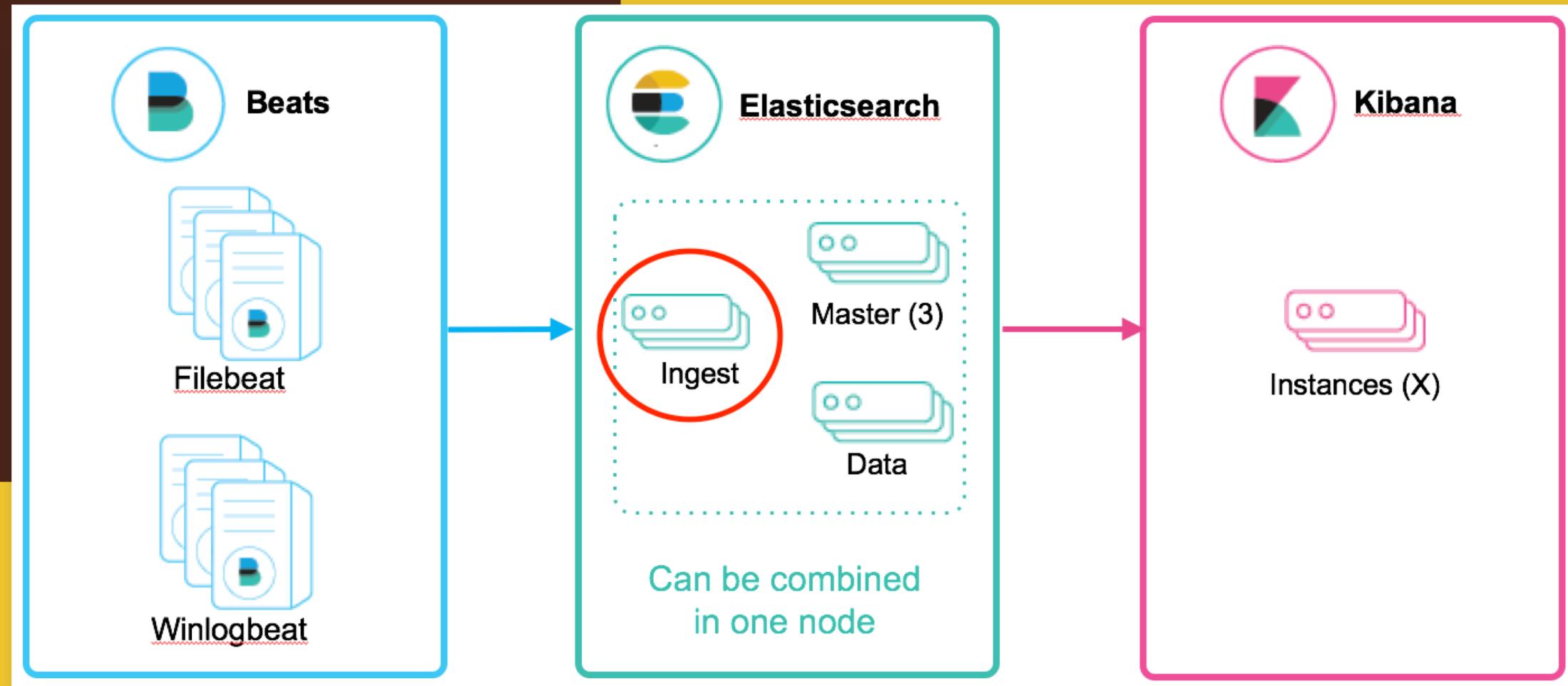
# Correlación de Logs

- Los eventos son unitarios, es algo que ocurrió en un determinado momento realizando una determinada acción. Correlar los logs permite entender una seguidilla de eventos que dan sentido a una acción más complicada.
- Logs:
  - **18:00hrs:** Se baten huevos, mantequilla con el azúcar
  - **18:10hrs:** Se agrega harina a la mezcla. Se continua batiendo
  - **18:14hrs:** Se vierte leche en la mezcla
  - **18:17hrs:** Se vacía en un bowl y coloca en el horno
  - **18:40hrs:** Se pincha la masa cocinada
  - **18:45hrs:** Se coloca sobre un plato

# Kill-Chain

- Es el orden presentado por Lockheed Martin sobre como se arman los ciberataques.





## MÓDULO 2: EXTRACCIÓN, PARSEO Y NORMALIZACIÓN

# Estructura del Módulo 2

- Formatos de Logs
- Formato logs: Servidores Web
- Limitaciones de los Logs
- Expresiones Regulares/GROK
- Esquema de procesamiento de Logs

# Formato de Logs

- Cada sistema, tiene su forma única de exportar logs.
  - *Líneas de texto*
  - *Multi-tipo*
  - *XML*
  - *Multi-línea*
  - *Timestamps variados*
  - *Key-Value*
  - *CSV*
  - *Etc...*
- Buscar la documentación es clave.
- Es casi como aprender un nuevo idioma.

# Logs IIS5.0

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2006-10-09 05:00:15
#Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes
2006-10-09 05:00:15 24.118.118.106 36A42160 SMTPSVC1 MEE-PDC 192.168.1.2 0 HELO - +36A42160 250 0 48 13 0 SMTP ----- 
2006-10-09 05:00:16 24.118.118.106 36A42160 SMTPSVC1 MEE-PDC 192.168.1.2 0 MAIL - +FROM:+<EldonpyzWestoncusk@sbcglobal.net> 250 0 57 45 0 SMTP ----- 
2006-10-09 05:00:16 24.118.118.106 36A42160 SMTPSVC1 MEE-PDC 192.168.1.2 0 RCPT - +TO:+<pamb@meelift.com> 250 0 29 27 0 SMTP ----- 
2006-10-09 05:00:19 24.118.118.106 36A42160 SMTPSVC1 MEE-PDC 192.168.1.2 0 DATA - +<4F5002F2.860022@web.de> 250 0 108 1399 1922 SMTP ----- 
2006-10-09 05:00:19 24.118.118.106 36A42160 SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - 36A42160 240 6219 68 4 0 SMTP ----- 
2006-10-09 05:00:42 192.168.1.247 notify.ossec.net SMTPSVC1 MEE-PDC 192.168.1.2 0 HELO - +notify.ossec.net 250 0 47 21 0 SMTP ----- 
2006-10-09 05:00:42 192.168.1.247 notify.ossec.net SMTPSVC1 MEE-PDC 192.168.1.2 0 MAIL - +From:+<ossecm@HULK> 250 0 36 24 16 SMTP ----- 
2006-10-09 05:00:42 192.168.1.247 notify.ossec.net SMTPSVC1 MEE-PDC 192.168.1.2 0 RCPT - +To:+<dbveto@meelift.com> 250 0 31 29 0 SMTP ----- 
2006-10-09 05:00:42 192.168.1.247 notify.ossec.net SMTPSVC1 MEE-PDC 192.168.1.2 0 DATA - <MEE-PDCfSDGAIWb9DY00001e05@mee-pdc.meelift.com> 250 0 132 29 
2006-10-09 05:00:42 192.168.1.247 notify.ossec.net SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - notify.ossec.net 240 78 68 4 0 SMTP ----- 
2006-10-09 05:00:50 192.168.1.22 REDBARRON SMTPSVC1 MEE-PDC 192.168.1.2 0 EHLO - +REDBARRON 250 0 275 14 93 SMTP ----- 
2006-10-09 05:00:50 192.168.1.22 REDBARRON SMTPSVC1 MEE-PDC 192.168.1.2 0 MAIL - +FROM:<Kiwisyslog@meelift.com> 250 0 47 34 0 SMTP ----- 
2006-10-09 05:00:50 192.168.1.22 REDBARRON SMTPSVC1 MEE-PDC 192.168.1.2 0 RCPT - +TO:<dbveto@meelift.com> 250 0 31 28 0 SMTP ----- 
2006-10-09 05:00:50 192.168.1.22 REDBARRON SMTPSVC1 MEE-PDC 192.168.1.2 0 DATA - <MEE-PDCccSN00ktmzmV00001e06@mee-pdc.meelift.com> 250 0 132 2413 531 
2006-10-09 05:00:50 192.168.1.22 REDBARRON SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - REDBARRON 240 1015 68 4 0 SMTP ----- 
2006-10-09 05:01:04 24.95.255.99 - SMTPSVC1 MEE-PDC 192.168.1.2 0 xxxx - +rr.com 500 0 32 11 0 SMTP ----- 
2006-10-09 05:01:04 24.95.255.99 - SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - - 240 375 68 4 16 SMTP ----- 
2006-10-09 05:01:19 70.114.247.230 - SMTPSVC1 MEE-PDC 192.168.1.2 0 xxxx - +rr.com 500 0 32 11 0 SMTP ----- 
2006-10-09 05:01:19 70.114.247.230 - SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - - 240 172 68 4 0 SMTP ----- 
2006-10-09 05:01:26 24.174.89.177 - SMTPSVC1 MEE-PDC 192.168.1.2 0 xxxx - +rr.com 500 0 32 11 0 SMTP ----- 
2006-10-09 05:01:26 24.174.89.177 - SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - - 240 188 68 4 0 SMTP ----- 
2006-10-09 05:01:33 80.64.22.8 - SMTPSVC1 MEE-PDC 192.168.1.2 0 xxxx - +sveta 500 0 32 10 0 SMTP ----- 
2006-10-09 05:01:33 80.64.22.8 sveta SMTPSVC1 MEE-PDC 192.168.1.2 0 HELO - +sveta 250 0 44 10 0 SMTP ----- 
2006-10-09 05:01:33 80.64.22.8 sveta SMTPSVC1 MEE-PDC 192.168.1.2 0 MAIL - +FROM:<malaquias@fu-berlin.de> 250 0 47 34 0 SMTP ----- 
2006-10-09 05:01:33 80.64.22.8 sveta SMTPSVC1 MEE-PDC 192.168.1.2 0 RCPT - +TO:<heyrmanmheyrman@meelift.com> 250 0 40 37 0 SMTP ----- 
2006-10-09 05:01:37 80.64.22.8 sveta SMTPSVC1 MEE-PDC 192.168.1.2 0 DATA - +<000b01c6eb60$0511fad0$4507a8c0@sveta> 250 0 122 22786 3297 SMTP ----- 
2006-10-09 05:01:37 80.64.22.8 sveta SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - sveta 240 4735 68 4 0 SMTP ----- 
2006-10-09 05:02:11 71.127.86.239 isyndicate.com SMTPSVC1 MEE-PDC 192.168.1.2 0 HELO - +isyndicate.com 250 0 47 19 0 SMTP ----- 
2006-10-09 05:02:11 71.127.86.239 isyndicate.com SMTPSVC1 MEE-PDC 192.168.1.2 0 MAIL - +FROM:<grazia@isyndicate.com> 250 0 46 33 0 SMTP ----- 
2006-10-09 05:02:11 71.127.86.239 isyndicate.com SMTPSVC1 MEE-PDC 192.168.1.2 0 RCPT - +TO:<jgrub@meelift.com> 250 0 30 27 0 SMTP ----- 
2006-10-09 05:02:11 71.127.86.239 isyndicate.com SMTPSVC1 MEE-PDC 192.168.1.2 0 DATA - +<000001c6eb5f$c56726d0$8c12a8c0@usbt> 250 0 122 1754 406 SMTP 
2006-10-09 05:02:11 71.127.86.239 isyndicate.com SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - isyndicate.com 240 500 68 4 0 SMTP ----- 
2006-10-09 05:02:46 72.185.9.146 - SMTPSVC1 MEE-PDC 192.168.1.2 0 xxxx - +cpe-72-185-9-146.tampabay.res.rr.com 500 0 32 41 0 SMTP ----- 
2006-10-09 05:02:46 72.185.9.146 - SMTPSVC1 MEE-PDC 192.168.1.2 0 QUIT - - 240 125 32 41 62 SMTP ----- 
2006-10-09 05:03:13 83.34.136.228 altimaxns.com SMTPSVC1 MEE-PDC 192.168.1.2 0 HELO - +altimaxns.com 250 0 47 18 0 SMTP ----- 
2006-10-09 05:03:13 83.34.136.228 altimaxns.com SMTPSVC1 MEE-PDC 192.168.1.2 0 MAIL - +FROM:<veste@altimaxns.com> 250 0 44 31 0 SMTP ----- 
2006-10-09 05:03:13 83.34.136.228 altimaxns.com SMTPSVC1 MEE-PDC 192.168.1.2 0 RCPT - +TO:<jheyrman@meelift.com> 250 0 33 30 0 SMTP ----- 
```

# Logs SonicWall

```
Jan 3 13:45:36 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:06" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23419 src=2.2
Jan 3 13:45:36 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:07" fw=1.1.1.1 pri=1 c=32 m=30 msg="Administrator login denied due to bad
Jan 3 13:45:36 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:07" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23420 src=2.2
Jan 3 13:45:37 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:07" fw=1.1.1.1 pri=6 c=1024 m=537 msg="Connection Closed" n=567996 src=192
Jan 3 13:45:37 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:08" fw=1.1.1.1 pri=6 c=1024 m=537 msg="Connection Closed" n=567997 src=192
Jan 3 13:45:39 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:10" fw=1.1.1.1 pri=6 c=1024 m=537 msg="Connection Closed" n=567999 src=192
Jan 3 13:45:39 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:10" fw=1.1.1.1 pri=6 c=1024 m=537 msg="Connection Closed" n=567999 src=1.1
Jan 3 13:45:40 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:10" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23421 src=2.2
Jan 3 13:45:40 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:10" fw=1.1.1.1 pri=1 c=32 m=30 msg="Administrator login denied due to bad
Jan 3 13:45:40 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:11" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23422 src=2.2
Jan 3 13:45:43 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:14" fw=1.1.1.1 pri=5 c=256 m=38 msg="ICMP packet dropped" n=22070 src=219.
Jan 3 13:45:43 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:14" fw=1.1.1.1 pri=6 c=1024 m=537 msg="Connection Closed" n=568000 src=219.
Jan 3 13:45:44 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:15" fw=1.1.1.1 pri=6 c=16 m=346 msg="IKE Initiator: Start Quick Mode (Phas
Jan 3 13:45:44 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:15" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23423 src=1.1
Jan 3 13:45:44 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:15" fw=1.1.1.1 pri=4 c=16 m=483 msg="Received notify: INVALID_ID_INFO" n=1
Jan 3 13:45:45 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:15" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23424 src=192
Jan 3 13:45:46 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:17" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23425 src=192
Jan 3 13:45:47 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:18" fw=1.1.1.1 pri=6 c=1024 m=537 msg="Connection Closed" n=568001 src=2.2
Jan 3 13:45:49 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:20" fw=1.1.1.1 pri=6 c=1024 m=537 msg="Connection Closed" n=568002 src=192
Jan 3 13:45:50 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:20" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23426 src=192
Jan 3 13:45:50 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:21" fw=1.1.1.1 pri=6 c=262144 m=98 msg="Connection Opened" n=23427 src=192
```

# Pregunta:

¿De qué serían estos logs?

```
14:03:19 192.168.2.187 [62]USER Administrator 331 0
14:03:19 192.168.2.187 [62]PASS - 530 1326
14:03:19 192.168.2.187 [62]USER Administrator 331 0
14:03:19 192.168.2.187 [62]PASS - 530 1326
14:03:19 192.168.2.187 [62]USER Administrator 331 0
14:03:20 192.168.2.187 [62]PASS - 530 1326
14:03:20 192.168.2.187 [62]USER Administrator 331 0
14:03:20 192.168.2.187 [62]PASS - 530 1326
14:03:20 192.168.2.187 [62]USER Administrator 331 0
14:03:20 192.168.2.187 [62]PASS - 530 1326
14:03:21 192.168.2.187 [62]USER Administrator 331 0
14:03:21 192.168.2.187 [62]PASS - 530 1326
14:37:52 10.1.2.35 [63]USER username 331 0
14:37:52 10.1.2.35 [63]PASS - 230 0
14:37:52 10.1.2.35 [63]CWD /dir 250 0
14:37:52 10.1.2.35 [63]CWD /dir/_mm 550 2
14:37:52 10.1.2.35 [63]CWD /dir/_notes 250 0
14:37:54 10.1.2.35 [63]CWD / 250 0
14:37:54 10.1.2.35 [63]MKD /dir/XYIZNWSK 257 0
14:37:54 10.1.2.35 [63]CWD /dir 250 0
14:37:54 10.1.2.35 [63]CWD / 250 0
14:37:54 10.1.2.35 [63]RMD /dir/XYIZNWSK 250 0
```

# ¿y estos?

# Formato de logs: Servidores Web

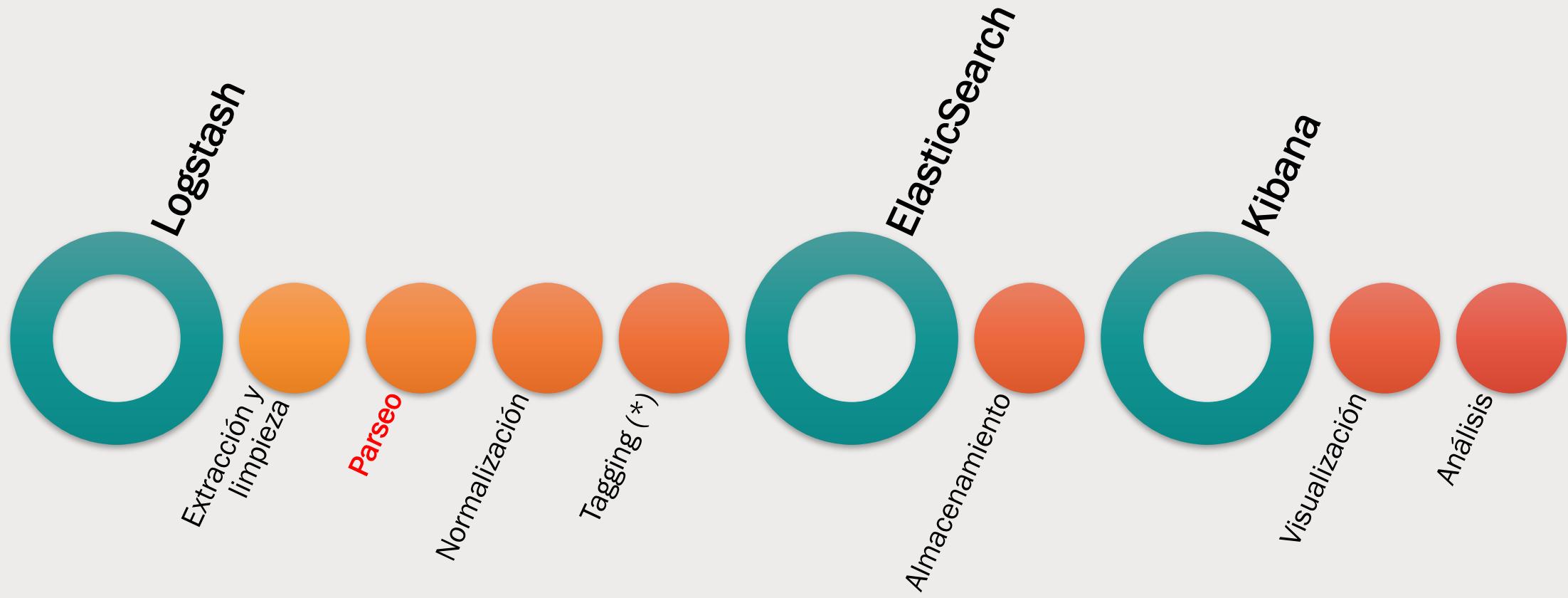
- Usualmente usan un formato llamado CLF (Common-Log-Format)
  - *Formato “común”*
  - *Los campos están definidos*
  - *El formato del timestamp es %d/%b/%Y:%H:%M:%S %z.*
  - *Utiliza “-” como para indicar que no hay data de ese estilo.*
  - *Parsearlo es bastante fácil y uno de los mejores casos.*
  - *Código de estado*

# Limitaciones de los Logs

- Solo funcionan si están habilitados.
- No dan toda la información que nos gustaría (ej: POST-HTTP).
- ES NECESARIO, saber la zona horaria del servidor.
- No siempre es trivial parsearlos.
- No siempre siguen la misma estructura.
- A veces pre-parsear es la única forma.

Wait... ¿parsear? ¿Qué?

# Esquema de Procesamiento de Logs



# Extracción y Limpieza

## ■ Extracción!

- Los logs están los sistemas
- En unix la mayor parte de los logs están en /var/log/
- En Windows... es más complejo extraer los EVT

## ■ Limpieza

- Los logs no siempre están en un formato... agradable (DNS Windows)
- A veces los datos necesitan un pre-procesamiento

# Parseo

- Es la transformación de un formato de logs a un formato de variables!

```
Aug 1 18:27:45  
knight sshd[20325]:  
Illegal user test from  
218.49.183.17
```

¿Qué paso?	Illegal user test
Ip de origen	218.49.183.17
Usuario	knight
Fecha	Aug 1 18:27:45
id	20325
Servicio	sshd

# Normalización

- Cuando se trabaja con distintos orígenes de dato, es importante que la variable que significa lo mismo en distintos logs tengan el mismo nombre o dimensión.

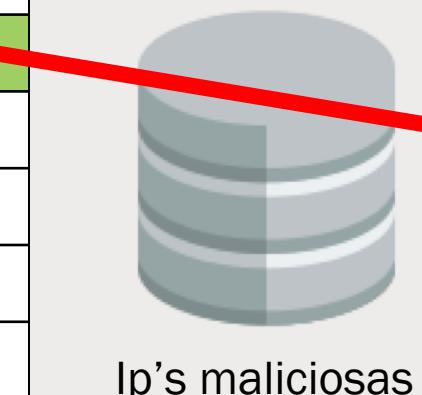
ip\_src == src\_ip == host == source\_ip      nombre

seg = ms = minutos      dimensión

# Tagging (no incluido en este taller)

- Durante la preparación de los datos a ser cargados, ciertas variables (por ejemplo source\_ip) son comparados con indicadores de compromiso, cmdbs, conocimientos previos para marcar el “log”.

¿Qué paso?	Illegal user test
Ip de origen	218.49.183.17
Usuario	knight
Fecha	Aug 1 18:27:45
id	20325
Servicio	sshd

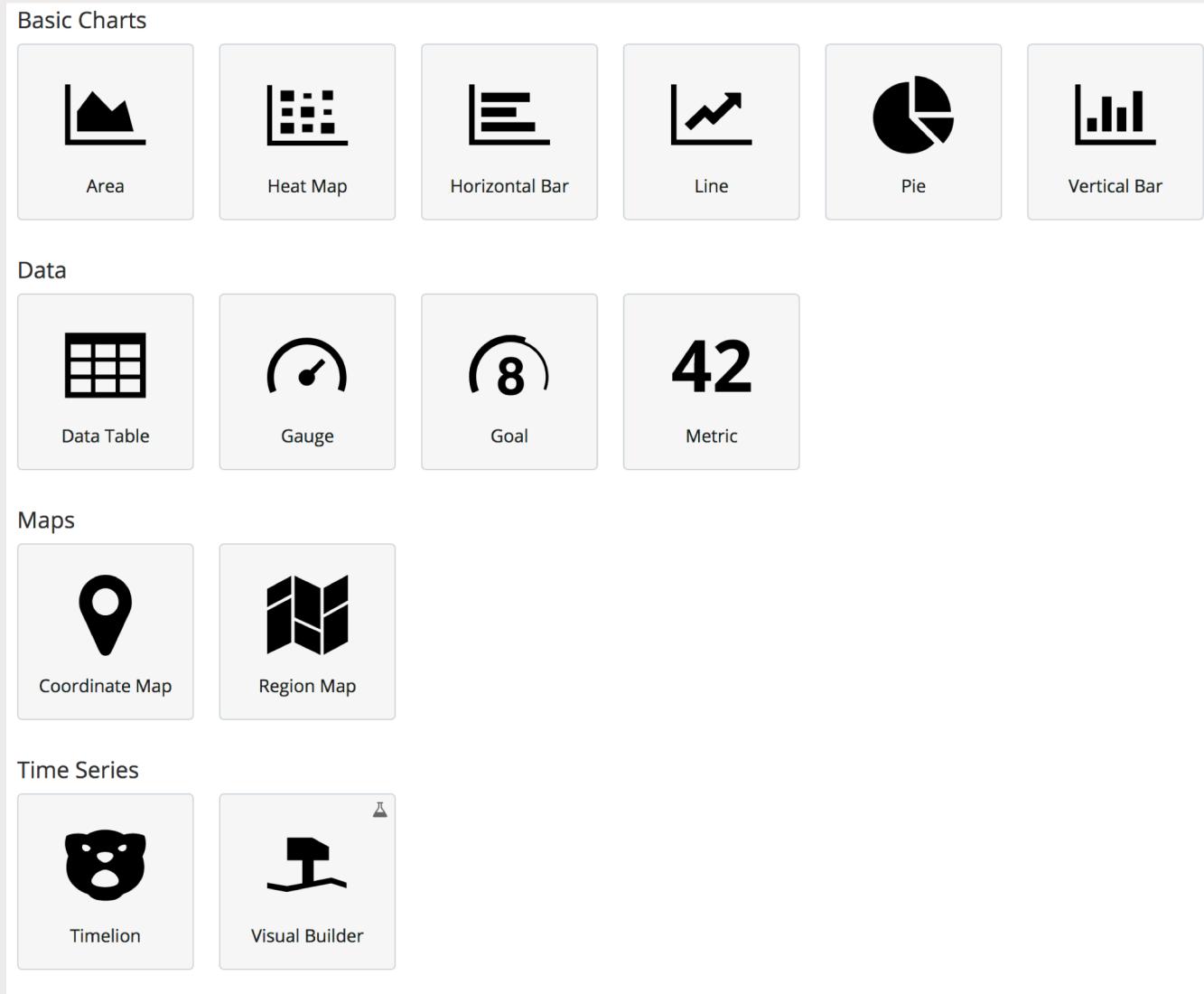


¿Qué paso?	Illegal user test
Ip de origen	218.49.183.17
Indicador	Malware IP
Usuario	knight
Fecha	Aug 1 18:27:45
id	20325
Servicio	sshd

# Almacenamiento

- La información en el formato requerido debe ser almacenado de una forma segura, confiable y que permita realizar búsquedas..
- Pensar en una tabla Excel es una buena forma (simplificada!) de ver los datos

timestamp	ip_src	user	id	service	Indicator	what
Aug 1 18:27:45	218.49.183.17	knight	20325	sshd	Malware IP	Illegal user test
Aug 1 18:27:46	218.49.183.17	knight	20325	sshd	Malware IP	Failed password for user test
Aug 1 18:27:46	-	knight	20325	sshd	-	Error: Could not get shadow information for NOUSER
...	...	...	...	...	...	...



# Visualización y Análisis

- Mediante la visualización de datos es posible detectar patrones, explicar comportamientos, encontrar rápidamente anomalías de forma mucho mas eficiente que directamente desde el log.
- En este taller usaremos Kibana

# Regular Expressions Tutorial #1

What is RegEx?

DETALLE DEL PARSEO CON  
EXPRESIONES REGULARES

# Expresiones Regulares

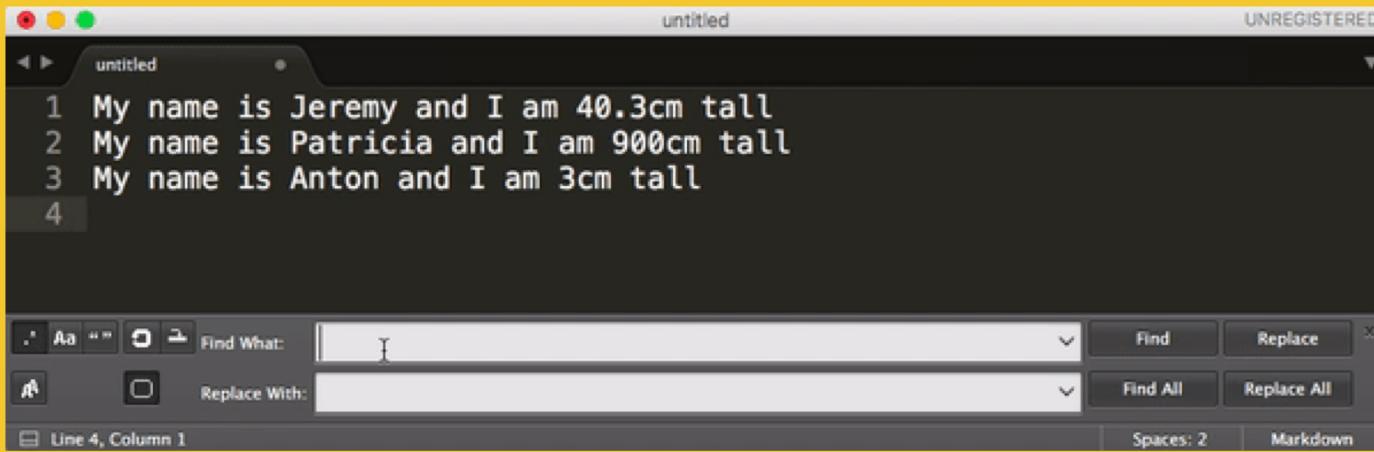
- Las expresiones regulares son difíciles, pero fáciles cuando se entienden.
- Son estructuras de lenguaje que permiten “seleccionar” patrones.
- Podríamos decir que es un lenguaje...
- Permite trabajar masivamente con textos.
- Es posible limpiar la data
- Aprenderemos lo básico!

# Sentencias importantes (1/2)

- ^ # Comienza con...
- \$ # Termina con...
- [a-z] # Selecciona minúsculas
- [A-Z] # Selecciona mayúsculas (se pueden combinar) -> [a-zA-Z]
- [0-9] # Todos los números entre el 0 y el 9
- . # Comodín de cualquier cosa excepto saltos de línea
- \* # Repite la secuencia 0 o muchas veces
- + # Repite la secuencia 1 o muchas veces
- ( .... ) # Grupos de captura! (importante)

# Sentencias importantes (2/2)

- \s # Selecciona un espacio en blanco
- \w # Selecciona cualquier letra (equivalente a [A-Za-z0-9\_])
- \d # Selecciona dígitos (equivalente a [0-9])
- \ # Un literal (por ejemplo para matchear "+")
- \t # Selecciona un TAB (→)
- \n # Selecciona un salto de línea
- (?<name>regex) # Grupo nombre para una expresión regular



```
1 My name is Jeremy and I am 40.3cm tall
2 My name is Patricia and I am 900cm tall
3 My name is Anton and I am 3cm tall
4
```

The screenshot shows a dark-themed text editor window titled "untitled". The status bar at the top right indicates "UNREGISTERED". The main text area contains four numbered lines of text. Below the text area is a toolbar with various icons and two search/replace input fields. The "Find What:" field contains a single character, and the "Replace With:" field is empty. The status bar at the bottom shows "Line 4, Column 1", "Spaces: 2", and "Markdown".

# LIMPIEMOS UN ARCHIVO...

# Genial! Me gustaron... ¿qué era el Grok?

- Es una forma “simplificada” para parsear archivos...
- Su estructura es la siguiente: %{GROK\_TYPE:variable}
- Permite definir estructuras más fáciles de implementar.
  
- Ejemplos:
  - %{SYSLOGTIMESTAMP:fecha}
  - %{WORD:palabras}
  - %{IPORHOST:ip\_o\_host}

<http://grokconstructor.appspot.com/do/match>

# Veamos el siguiente LOG.

```
Aug 1 18:27:45 knight sshd[20325]: Illegal user test from 218.49.183.17
```

Regex:

```
^(?<mes>\w+)\s+(?<dia>\d+)\s(?<hora>\d+):\(?:?<minutos>\d+)\?:(?<segundos>\d+)\s(?<user>\w+)\s(?<servicio>\w+)\[(?<id>\d+)\]\:\s(?<quepaso>.*)
```

Grok:

```
%{SYSLOGTIMESTAMP:fecha} %{WORD:usuario} %{WORD:servicio}\[%{NUMBER:id}\]\%{GREEDYDATA:quepaso}
```

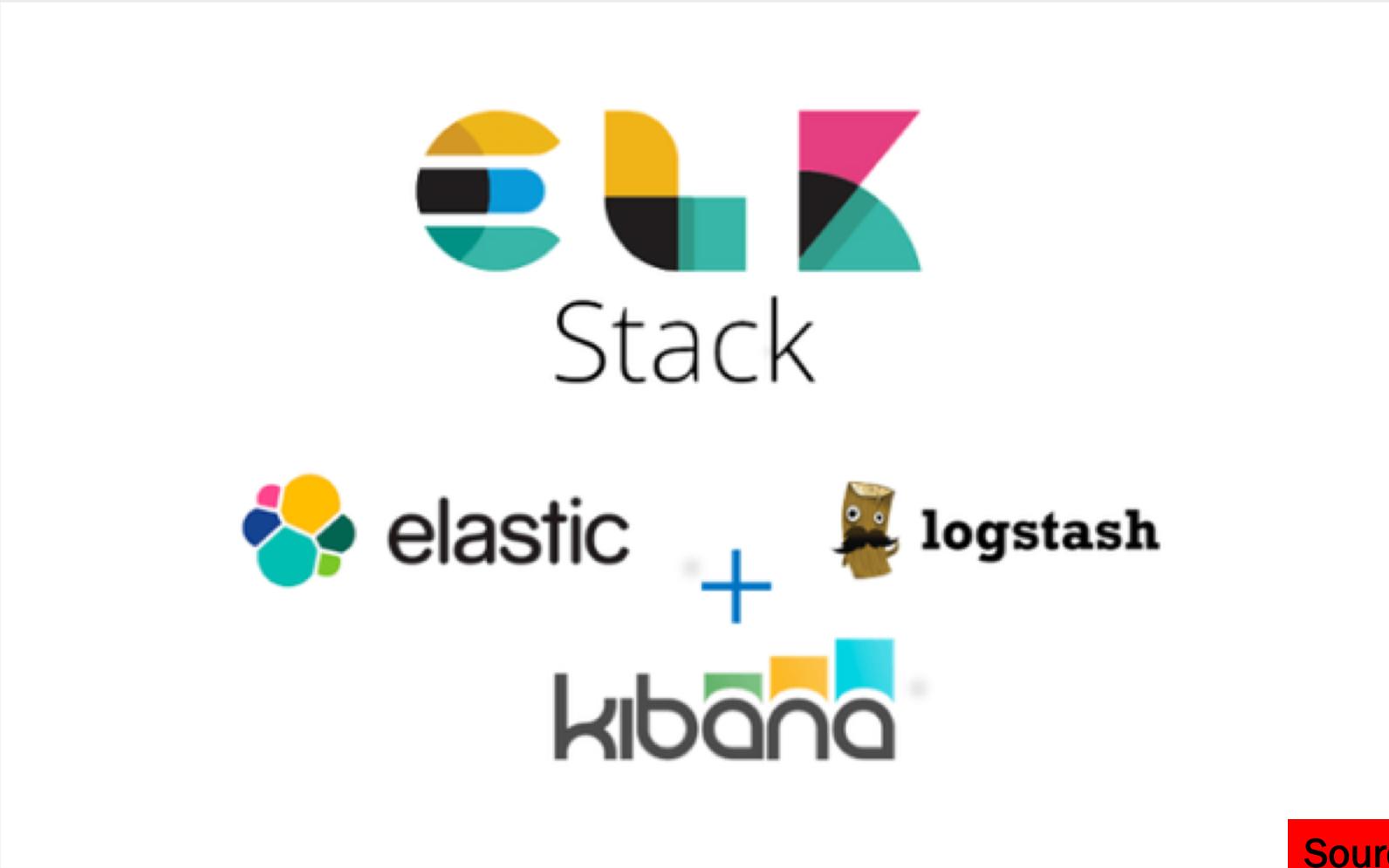


# MÓDULO 3: PREPARACIÓN DEL LABORATORIO

# Estructura del Módulo 3

- ¿Qué es ELK?
- ¿Qué es Logstash?
- ¿Qué es ElasticSearch?
- ¿Qué es Kibana?
- Entendiendo Logstash, ElasticSearch, Kibana y como se combinan

# ¿Qué es ELK?



Source: Quora.com

# ¿Qué es Logstash?

- Un procesador de información mediante pipeline.
- Programado en Java (⌚)
- Servirá para parsear, normalizar y cargar los datos.
- El concepto de **mensaje** (*message*) es fundamental.
  
- El pipeline se divide en fases
  - *Input:* Entrada de la información
  - *Filter:* Manejo, parseo, normalización, tageo, de cada línea de código
  - *Output:* Qué hacer con el mensaje

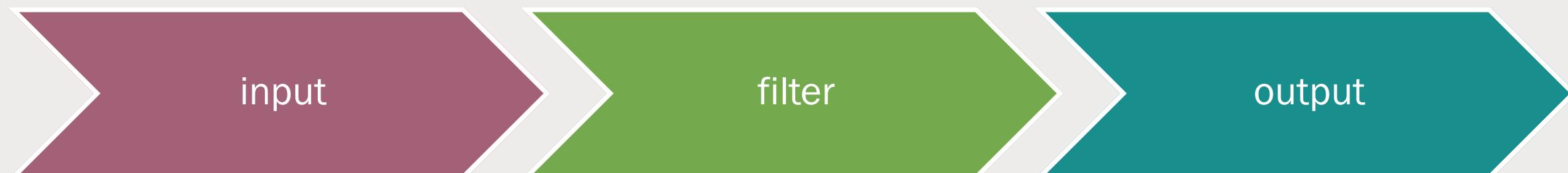
# Ejemplo de configuración

```
Input {  
    file { path => "/var/log/syslog" }  
}  
  
filter {  
    grok {  
        match => { "message" => "%{SYSLOGTIMESTAMP:timestamp}%{GREEDYDATA:log}" }  
    }  
}  
  
output {  
    stdout { codec => rubydebug }  
}
```

# Cada línea de log es un “message”...

Un log

```
Aug 1 18:27:45 knight sshd[20325]: Illegal user test from 218.49.183.17
Aug 1 18:27:46 knight sshd[20325]: Failed password for illegal user test from 218.49.183.17 port 48849 ssh2
Aug 1 18:27:46 knight sshd[20325]: error: Could not get shadow information for NOUSER
Aug 1 18:27:48 knight sshd[20327]: Illegal user guest from 218.49.183.17
Aug 1 18:27:49 knight sshd[20327]: Failed password for illegal user guest from 218.49.183.17 port 49090 ssh2
```



- **file** => cada línea de log
- **grok** => el mensaje se parsea
- **stdout** => Muestra en la consola el resultado

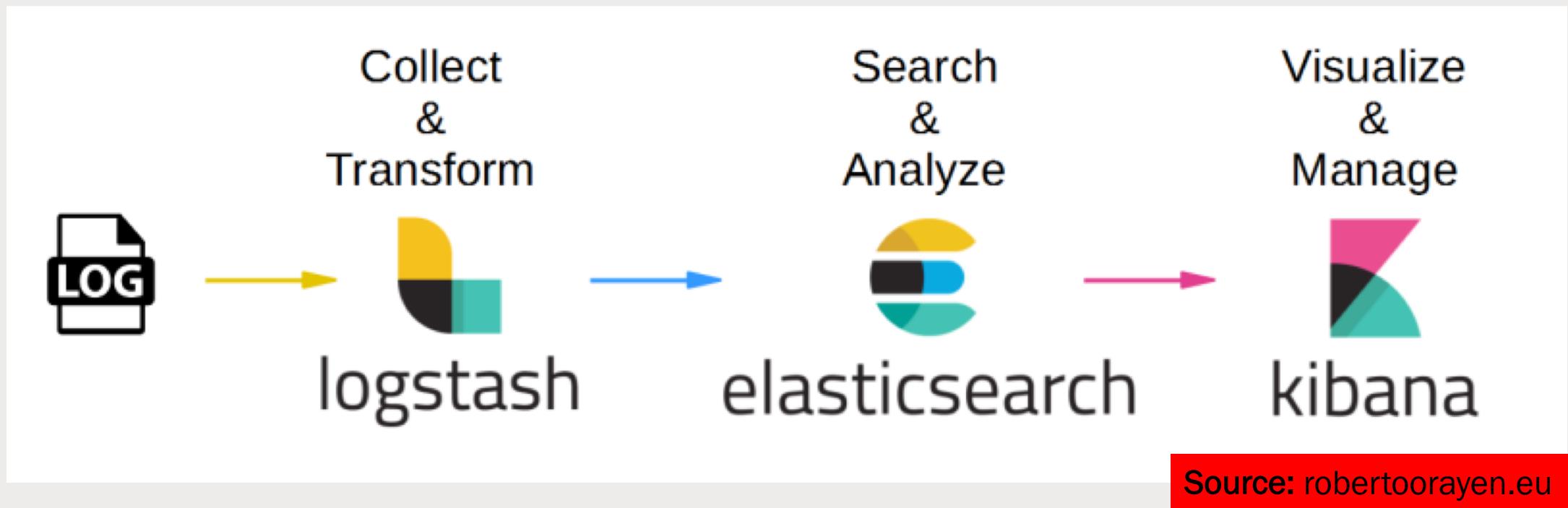
# ¿Qué es ElasticSearch?

- Es una base de datos full-text search
- Basado en REST
- Almacena en algo llamado “documentos”
- Utiliza json para sus archivos
- Soporte Apache Lucene
- Cada dato (llamado documento, doc), se guarda en un índice (index)
- Utilizado por:
  - *Wikipedia*
  - *The Guardian*
  - *Stack Overflow*
  - *Github*
  - *Entre muchos más...*

# ¿Qué es Kibana?

- Una interfaz gráfica para “visualizar” los datos que están almacenados en los índices.
- Es intuitiva y fácil de utilizar, aprenderemos lo básico en este taller.
- Consulta directamente vía la API de ElasticSearch
- Contiene visualizadores y la utilizaremos para analizar la data
- Se utiliza con un browser.

# Entendiendo Logstash, ElasticSearch, Kibana y como se combinan



Page Gauge [...]

Load Gauge [Metricbeat...]

Inbound Traffic [Metric...]

Outbound Traffic [Metri...]

Packetloss [Metricbeat...]

CPU Usage  
25.78%

Memory Usage  
54%

5m Load  
2.51

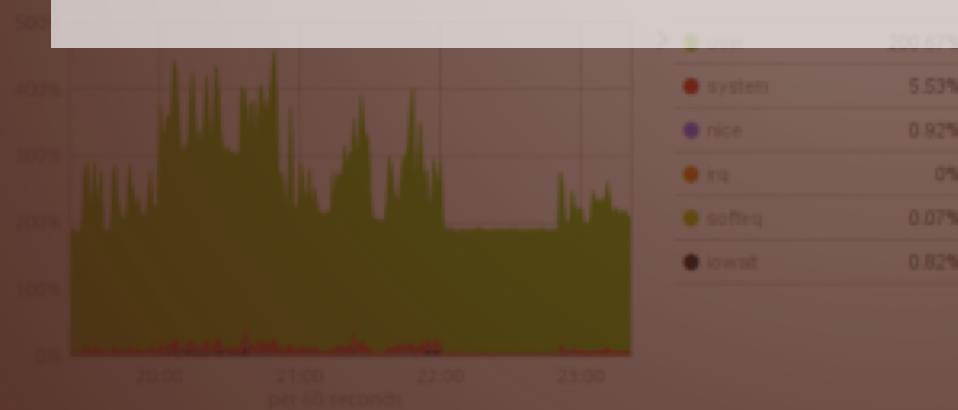
Inbound Traffic  
**2.8KB/s**  
Total Transferred 4.2GB

Outbound Traffic  
**318.0B/s**  
Total Transferred 202.6MB

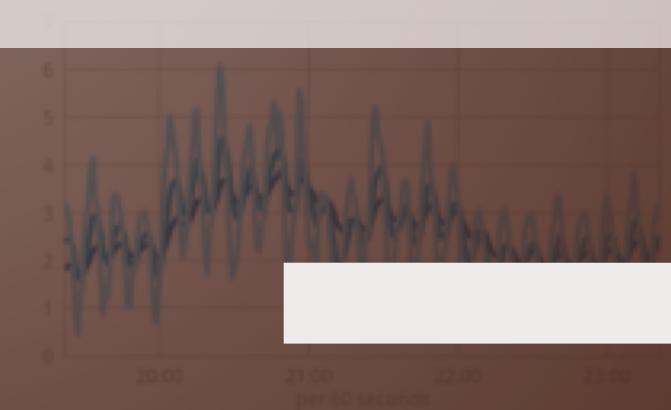
In Packetloss  
**2,666**  
Out Packets 0

# MÓDULO 4: ANÁLISIS CON ELK

CPU Usage [Metricbeat System]



System Load [Metricbeat System]



Realizamos una carga de datos, analizemos el Logstash que usamos.

(Ver el que está en sus computadores)

	Data Type	Count
<b>ts</b>	float64	2048442
<b>uid</b>	object	2048442
<b>id.orig_h</b>	object	2048442
<b>id.orig_p</b>	int64	2048442
<b>id.resp_h</b>	object	2048442
<b>id.resp_p</b>	int64	2048442
<b>trans_depth</b>	int64	2048442
<b>method</b>	object	2047566
<b>host</b>	object	2042003
<b>uri</b>	object	2047566
<b>referrer</b>	object	382520
<b>user_agent</b>	object	1977097
<b>request_body_len</b>	int64	2048442
<b>response_body_len</b>	int64	2048442
<b>status_code</b>	float64	2011424
<b>status_msg</b>	object	2011424
<b>info_code</b>	float64	2
<b>info_msg</b>	object	2
<b>filename</b>	float64	0
<b>tags</b>	object	2048442
<b>username</b>	object	7146
<b>password</b>	float64	0
<b>proxied</b>	object	1154
<b>orig_fuids</b>	object	133222
<b>orig_mime_types</b>	object	133222
<b>resp_fuids</b>	object	705213
<b>resp_mime_types</b>	object	705213

# Datos en http.log

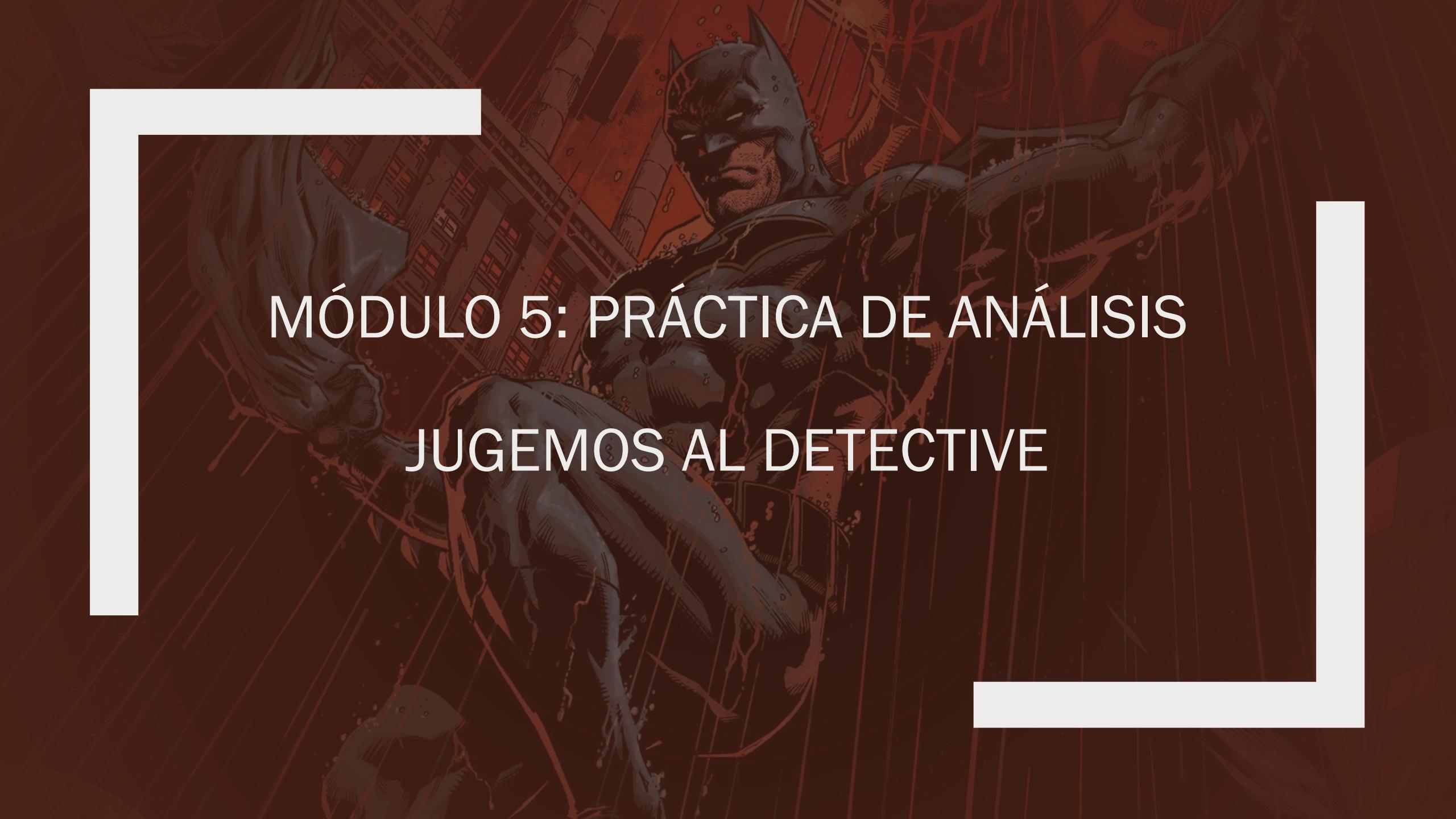
- **Fecha de Inicio:** 16 de Marzo 2012
- **Fecha de término:** 17 de Marzo 2012
- **Formato de TZ:** Unix MS
- **Estilo de Log:** Líneas de texto

# Grok que parsea estos datos

```
%{NUMBER:ts}\t%{GREEDYDATA:uid}\t%{IP:id.orig_h}\t%{NUMBER:id.orig_p}\t%{IP:id.resp_h}\t%{NUMBER:id.resp_p}\t%{GREEDYDATA:trans_depth}\t%{GREEDYDATA:method}\t%{GREEDYDATA:server_host}\t%{GREEDYDATA:uri}\t%{GREEDYDATA:referrer}\t%{GREEDYDATA:user_agent}\t%{NUMBER:request_body_len}\t%{GREEDYDATA:response_body_len}\t%{GREEDYDATA:status_code}\t%{GREEDYDATA:status_msg}\t%{GREEDYDATA:info_code}\t%{GREEDYDATA:info_msg}\t%{GREEDYDATA:filename}\t%{GREEDYDATA:tags}\t%{GREEDYDATA:username}\t%{GREEDYDATA:pass}\t%{GREEDYDATA:proxied}\t%{GREEDYDATA:orig_fuids}\t%{GREEDYDATA:orig_mime_types}\t%{GREEDYDATA:resp_fuids}\t%{GREEDYDATA:resp_mime_types}
```

A crear visualizaciones para trabajar!

<https://bit.ly/2yPhN4u>



# MÓDULO 5: PRÁCTICA DE ANÁLISIS

## JUGEMOS AL DETECTIVE

# Ejercicio 1:

- El equipo nos solicita entender los datos que tenemos disponibles para comenzar a familiarizarnos con nuestro Dashboard, piden responder las siguientes preguntas:
  - *¿Cuál fue la IP de Origen que generó más solicitudes?*
  - *¿Cuál fue el User-Agent más utilizado?*
  - *¿Cuál fue el recurso más solicitado?*
  - *¿Cuál fue la respuesta más común del servidor? ¿Qué podemos concluir de esto?*

# Ejercicio 2:

- Desde ciberseguridad nos indican que se descubrió una web shell en PHP (c99.php) que permitió a un atacante tomar control del servidor. El analista senior solicita la siguiente información para analizar el caso.
  - *¿Qué dirección IP utilizó satisfactoriamente la Shell?*
  - *¿Cuál fue el primer momento en que la Shell fue accedida?*
  - *¿En qué URL encontró la Shell el usuario?*
  - *¿Existen más ubicaciones donde la Shell esté presente? ¿Cuáles?*

# Ejercicio 3:

- Llego nueva información, al parecer el caso es más complejo de lo que se creía. Si bien TI eliminó el backdoor (c99.php) necesitamos más información del atacante. Favor responde las siguientes preguntas.
  - *¿Se vio tráfico extraño en el puerto 5357 desde esta IP ¿Logró acceder a algún recurso en este puerto?*
  - *¿Se llevó algún archivo ejecutable (**Mimetype: application/x-dosexec**)?*
  - *¿A qué hora se lo llevo?*
  - *¿Quién más descargo este ejecutable?*

# Ejercicio 4:

- Se cree que la persona que atacó a la compañía utilizó alguna herramienta de escaneo automático. Necesitamos entender como entró!
  - *¿Qué herramienta utilizó? Nombre dos (tip: un scanner y un spider).*
  - *¿Alguien más utilizó estas herramientas?*
  - *Utilizando el spider, cuantas URL encontró satisfactoriamente?*

# Ejercicio 5:

- Se cree que la persona que atacó a la compañía utilizó alguna herramienta de escaneo automático. Necesitamos entender como entró!
  - *¿Qué herramienta utilizó? Nombre dos.*
  - *¿Alguien más utilizó estas herramientas?*
  - *Aparecen muchos errores 500. ¿Qué estaba intentando hacer el atacante?*

# CIERRE

gettyimages®  
BraunS