



Computación Forense

Análisis de Logs y Evidencias

Clase 3b

Profesor: Ing. Alex Araya Rojas, MT
CISSP, CISM

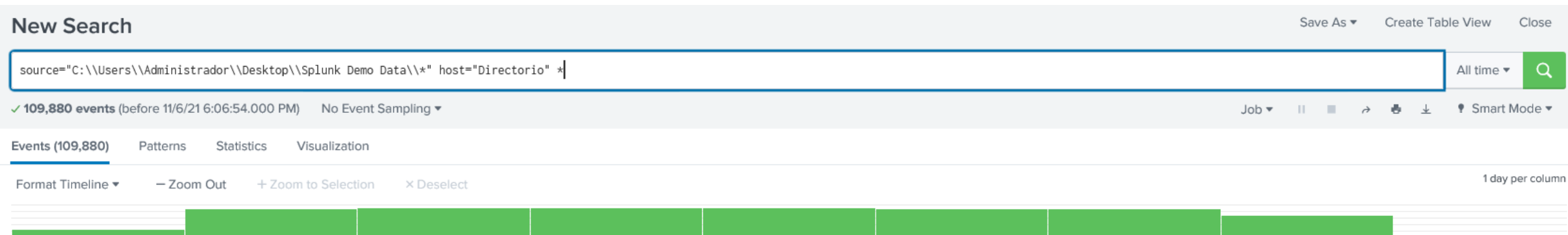
Análisis de Logs y Evidencias

- **Logs**

- Uno de los grandes problemas que experimentan los analizadores forenses cuando analizan logs es la gran cantidad de registros que se nos presentan.
- Si a esto le sumamos la diversidad de fuentes (firewall, logs de sistema operativo, IPS, etc.) y la poca estandarización de los campos que los conforman, solo termina confirmando lo difícil de la tarea.
- La utilización de herramientas que nos permitan correlacionar, buscar y ordenar los logs se vuelve fundamental, el lab de esta semana tiene este propósito.

Análisis de Logs y Evidencias

- Logs
- Pasar de analizar miles de eventos en total a una segregación por horas o minutos de forma dinámica le provee al investigador una fuente de información muy valiosa.



Análisis de Logs y Evidencias

- Logs
- Pasar de analizar miles de eventos en total a una segregación por horas o minutos de forma dinámica le provee al investigador una fuente de información muy valiosa.

New Search

source="Fortigate" sourcetype="Fortigate"

All time

98 events (before 11/7/21 1:22:20.000 PM) No Event Sampling

Job

Smart Mode

Events (98) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 second per column

List Format 20 Per Page

Prev 1 2 3 4 5 Next

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

i	Time	Event
>	11/7/21 1:22:19.000 PM	Nov 7 13:22:19 10.17.0.1 date=2021-11-07 time=13:22:18 devname="Forti-Alex" devid="FGT50E3U16016229" logid="1059028704" type="utm" subtype="app-ctrl" eventtype="signature" level="information" vd="root" eventtime=1636312940386206880 tz="-0600" appid=41469 srcip=10.17.0.207 dstip=20.42.73.25 srcport=50070 dstport=443 srcintf="lan4" srcintfrole="lan" dstintf="wan1" dstintfrole="wan" proto=6 service="SSL" direction="outgoing" policyid=1 sessionid=660521 applist="default" action="pass" appcat="Collaboration" app="Microsoft.Portals" hostname="v10.events.data.microsoft.com" incidentserialno=620069137 url="/" msg="Collaboration: Microsoft.Portal," apprisk="elevated" scertcname="*.events.data.microsoft.com" scertissuer="Microsoft Secure Server CA 2011" host = 10.17.0.1 source = Fortigate sourcetype = Fortigate

Análisis de Logs y Evidencias

- Logs

New Search

Save As ▾Create Table ViewClose


source="Fortigate" sourcetype="Fortigate" crhoy

All time ▾

✓ 6 events (before 11/7/21 1:25:22.000 PM) No Event Sampling ▾

Events (6)PatternsStatisticsVisualization

Format Timeline ▾Zoom OutZoom to SelectionDeselect



List ▾Format20 Per Page ▾

< Hide FieldsAll Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a action 1

a app 2

a appcat 2

appid 2

a applist 1

i

Time

Event

>

11/7/21
1:25:13.000 PM

Nov 7 13:25:13 10.17.0.1 date=2021-11-07 time=13:25:13 devname="Forti-Alex" devid="FGT50E3U1" l="information" vd="root" eventtime=1636313114157376920 tz="-0600" appid=40568 srcip=10.17.0.1 stntf="wan1" dstntfrole="wan" proto=6 service="SSL" direction="incoming" policyid=1 sessionid="www.crhoy.com" incidentserialno=2008444557 url="/" msg="Web.Client: HTTPS.BROWSER," a host = 10.17.0.1 source = Fortigate sourcetype = Fortigate

>

11/7/21
1:25:13.000 PM

Nov 7 13:25:13 10.17.0.1 date=2021-11-07 time=13:25:13 devname="Forti-Alex" devid="FGT50E3U1" l="information" vd="root" eventtime=1636313114157133480 tz="-0600" appid=15895 srcip=10.17.0.1 stntf="wan1" dstntfrole="wan" proto=6 service="SSL" direction="outgoing" policyid=1 sessionid="www.crhoy.com" incidentserialno=2008444556 url="/" msg="Network.Service: SSL," apprisk="el host = 10.17.0.1 source = Fortigate sourcetype = Fortigate

☐ hostname ▾www.crhoy.com

☐ incidentserialno ▾2008444557

☐ level ▾information

☐ logid ▾1059028704

☐ msg ▾Web.Client: HTTPS.BROWSER,

☐ policyid ▾1

☐ proto ▾6

☐ service ▾SSL

☐ sessionid ▾660958

☐ srcintf ▾lan4

☐ srcintfrole ▾lan

☐ srcip ▾10.17.0.207

Análisis de Logs y Evidencias

- **Evidencia**

- Para entender el proceso de análisis de la evidencia también preparamos un laboratorio.
- Este ejercicio le permitirá extraer el contenido de una llave usb y a extraer la memoria RAM de un equipo en ejecución para realizar análisis de dicha evidencia con herramientas forenses para ir generando un listado de hallazgos que le permitan generar un informe del caso.

Análisis de Logs y Evidencias

- **Evidencia**

- Herramientas como Autopsy y FTK están dentro de las elegidas para estos laboratorios y ambas muy reconocidas en el mundo forense.
- El análisis de los archivos de evidencia, la generación de líneas de tiempo y ubicaciones geográficas son vitales en estos procesos y trataremos de recrearlas para su aprendizaje.



Gracias