

In-Class Lab #6

Opening pcap file w/ wireshark

2022-03-21-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.19.14	188.166.154.118	TCP	66	62179 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.183655	188.166.154.118	10.0.19.14	TCP	66	80 → 62179 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.183794	10.0.19.14	188.166.154.118	TCP	60	62179 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
4	0.186751	10.0.19.14	188.166.154.118	HTTP	365	GET / HTTP/1.1
5	0.365907	188.166.154.118	10.0.19.14	TCP	60	80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=0
6	0.484243	188.166.154.118	10.0.19.14	TCP	1442	80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=13
7	0.493025	188.166.154.118	10.0.19.14	TCP	1442	80 → 62179 [ACK] Seq=1389 Ack=312 Win=64128 Len=0
8	0.493089	10.0.19.14	188.166.154.118	TCP	60	62179 → 80 [ACK] Seq=312 Ack=2777 Win=131840 Len=0
9	0.675897	188.166.154.118	10.0.19.14	TCP	1442	[TCP Previous segment not captured] 80 → 62179
10	0.676020	10.0.19.14	188.166.154.118	TCP	66	[TCP Dup ACK 8#1] 62179 → 80 [ACK] Seq=312 Ack=
11	0.679449	188.166.154.118	10.0.19.14	TCP	1442	80 → 62179 [ACK] Seq=15269 Ack=312 Win=64128 Len=0
12	0.679565	10.0.19.14	188.166.154.118	TCP	66	[TCP Dup ACK 8#2] 62179 → 80 [ACK] Seq=312 Ack=

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bi
> Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: C
> Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.
> Transmission Control Protocol, Src Port: 62179, Dst Port: 80, S

0000 2c 54 2d 2f 13 5c 00 60 52 b7 33 0f 08 00 45 00 ,T-/.\\.
0010 00 34 9c be 40 00 80 06 e9 da 0a 00 13 0e bc a6 .4..@..
0020 9a 76 f2 e3 00 50 0e 81 a4 2b 00 00 00 00 80 02 .v...P..
0030 fa f0 5a 14 00 00 02 04 05 b4 01 03 03 08 01 01 ..Z....
0040 04 02 ..

Exporting as .csv format

2022-03-21-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

Destination Protocol Length Info

Destination	Protocol	Length	Info
188.166.154.118	TCP	66	62179 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
10.0.19.14	TCP	66	80 → 62179 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
188.166.154.118	TCP	60	62179 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
188.166.154.118	HTTP	365	GET / HTTP/1.1
10.0.19.14	TCP	60	80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=0
10.0.19.14	TCP	1442	80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=13
10.0.19.14	TCP	1442	80 → 62179 [ACK] Seq=1389 Ack=312 Win=64128 Len=0
10.0.19.14	TCP	60	62179 → 80 [ACK] Seq=312 Ack=2777 Win=131840 Len=0
10.0.19.14	TCP	1442	[TCP Previous segment not captured] 80 → 62179
188.166.154.118	TCP	66	[TCP Dup ACK 8#1] 62179 → 80 [ACK] Seq=312 Ack=
188.166.154.118	TCP	1442	80 → 62179 [ACK] Seq=15269 Ack=312 Win=64128 Len=0
188.166.154.118	TCP	66	[TCP Dup ACK 8#2] 62179 → 80 [ACK] Seq=312 Ack=

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bi
> Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: C
> Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.
> Transmission Control Protocol, Src Port: 62179, Dst Port: 80, S

0000 2c 54 2d 2f 13 5c 00 60 52 b7 33 0f 08 00 45 00 ,T-/.\\.
0010 00 34 9c be 40 00 80 06 e9 da 0a 00 13 0e bc a6 .4..@..
0020 9a 76 f2 e3 00 50 0e 81 a4 2b 00 00 00 00 80 02 .v...P..
0030 fa f0 5a 14 00 00 02 04 05 b4 01 03 03 08 01 01 ..Z....
0040 04 02 ..

Successfully imported to splunk to perform search

splunk>enterpriseApps Jackson YuanMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboardsSearch & Reporting

New SearchSave AsCreate Table ViewClose

source="Lab 6.csv" host="VMWindows" sourcetype="csv"All time

16,296 events (before 10/20/22 11:48:50.000 PM)No Event SamplingJobSmart Mode

Events (16,296)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect1 hour per column

ListFormat50 Per Page12345678Next

Hide FieldsAll Fields

SELECTED FIELDSa host 1a source 1a sourcetype 1

INTERESTING FIELDS# date_hour 1# date_mday 1

i	Time	Event
>	10/20/22 11:48:46.000 PM	"539", "74.253273", "10.0.19.9", "10.0.19.14", "NTP", "162", "NTP Version 3, server" host = VMWindows source = Lab 6.csv sourcetype = csv
>	10/20/22 11:48:46.000 PM	"538", "74.251671", "10.0.19.14", "10.0.19.9", "NTP", "162", "NTP Version 3, client" host = VMWindows source = Lab 6.csv sourcetype = csv
>	10/20/22 11:48:46.000 PM	"537", "37.403519", "10.0.19.14", "20.189.173.15", "TCP", "60", "62181 > 443 [ACK] Seq=2265 Ack=4864 Win=131328 Len=0" host = VMWindows source = Lab 6.csv sourcetype = csv

Executive Summary

User Patrick Zimmerman was infected by a Bokbot malware

Details

Victim Patrick’s mac address for his computer

ListFormat50 Per Page

i	Time	Event
>	10/20/22 8:48:19.000 AM	"9019", "6664.638045", "PERIPHER_b7:33:0f", "Dell_f8:48:19", "ARP", "60", "10.0.19.14 is at 00:60:52:b7:33:0f" host = VMWindows source = Lab 6.csv sourcetype = csv

Infected host name

>	10/20/22 8:48:19.000 AM	"16124", "22438.790353", "10.0.19.9", "10.0.19.14", "LDAP", "238", "SASL GSS-API Integrity: searchResEntry(6) ""CN=DESKTOP-5Q53D5D,CN=Computers,DC=burnincand1e,DC=com"" searchResDone(6) success [4 results]" host = VMWindows source = Lab 6.csv sourcetype = csv
---	-------------------------	---

Ip address for patricks computer is 10.0.18.14 as per screenshots above

Indicators of Compromise

>	10/20/22 11:48:46.000 PM	"498", "24.690866", "188.166.154.118", "10.0.19.14", "TCP", "678", "80" > 62179 [PSH, ACK] Seq=392805 Ack=312 Win=64128 Len=624 [TCP segment of a reassembl
		ed PDU]"
		host = VMWindows source = Lab 6.csv sourcetype = csv

← → ↻ virustotal.com/gui/ip-address/188.166.154.118



188.166.154.118



8 security vendors flagged this IP address as malicious

188.166.154.118 (188.166.0.0/16)
AS 14061 (DIGITALOCEAN-ASN)

Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY 6

Security Vendors' Analysis

Antiy-AVL	Malicious	BitDefender	Phishing
CMC Threat Intelligence	Malware	Comodo Valkyrie Verdict	Malware
CRDF	Malicious	ESET	Malware
Fortinet	Malware	G-Data	Phishing
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean

>	10/20/22 11:48:46.000 PM	"514", "26.123656", "157.245.142.66", "10.0.19.14", "TCP", "60", "443" > 62180 [ACK] Seq=1755 Ack=529 Win=64128 Len=0"
		host = VMWindows source = Lab 6.csv sourcetype = csv

← → ↻ virustotal.com/gui/ip-address/157.245.142.66/detection



157.245.142.66



9 security vendors flagged this IP address as malicious

157.245.142.66 (157.245.0.0/16)
AS 14061 (DIGITALOCEAN-ASN)

Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY 4

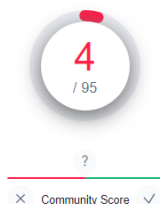
Security Vendors' Analysis

Avira	Malware	BitDefender	Malware
CRDF	Malicious	ESTsecurity	Malicious
Fortinet	Malware	G-Data	Malware
Sophos	Malware	Viettel Threat Intelligence	Malicious
Webroot	Malicious	Forcepoint ThreatSeeker	Suspicious

>	10/20/22 8:48:19.000 AM	"2516","116.877761","160.153.32.99","10.0.19.14","TCP","1442","443 > 62195 [ACK] Seq=9225 Ack=407 Win=15872 Len=1388 [TCP segment of a reassembled PD UJ]" host = VMWindows source = Lab 6.csv sourcetype = csv
i	Time	Event
>	10/20/22 8:48:19.000 AM	"566","87.046609","10.0.19.9","10.0.19.14","DNS","95","Standard query response 0x92de A suncoastpinball.com A 160.153.32.99" host = VMWindows source = Lab 6.csv sourcetype = csv
>	10/20/22 8:48:19.000 AM	"564","86.977912","10.0.19.14","10.0.19.9","DNS","79","Standard query 0x92de A suncoastpinball.com" host = VMWindows source = Lab 6.csv sourcetype = csv



suncoastpinball.com



4 security vendors flagged this domain as malicious

suncoastpinball.com

Registrar
GoDaddy.com, LLC

Creation
4 years i

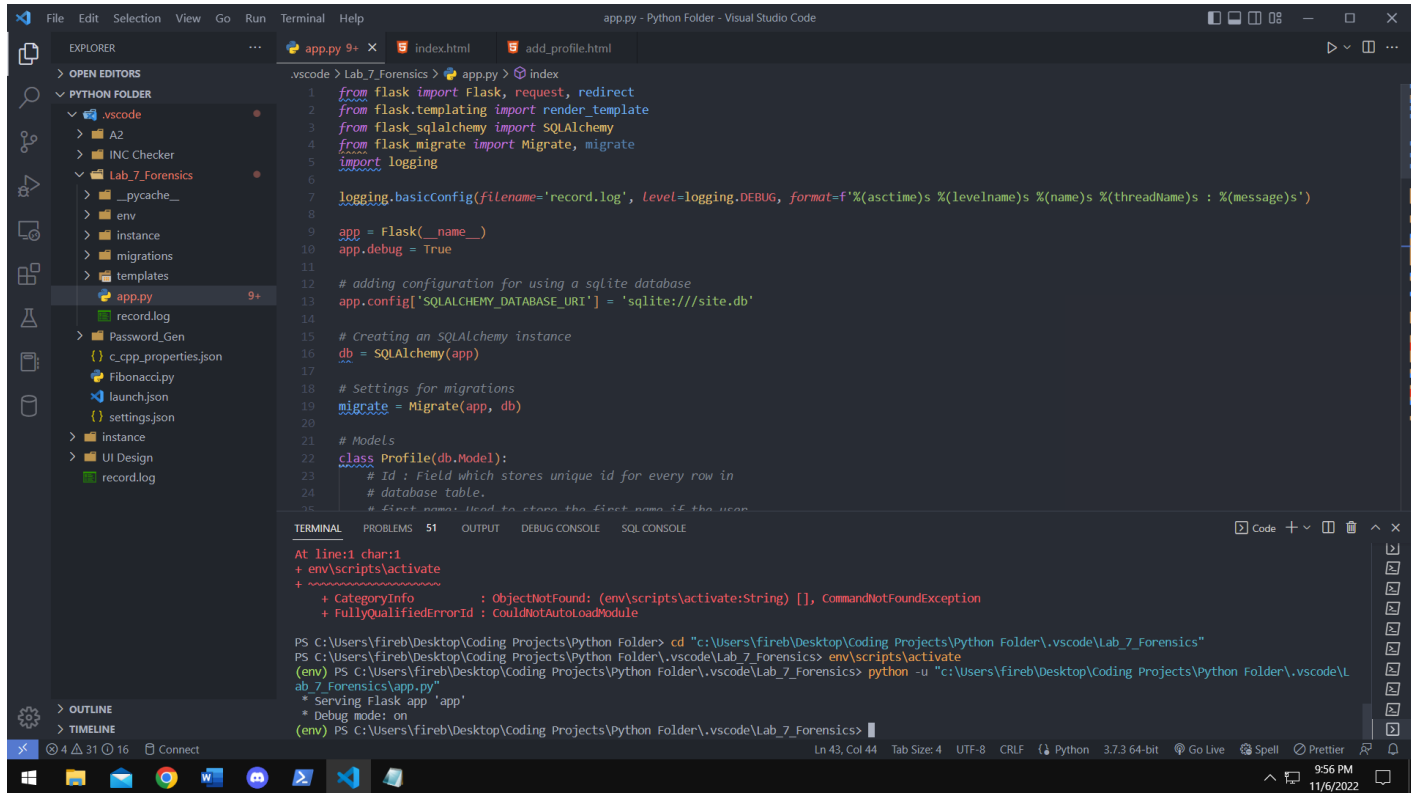
DETECTION DETAILS RELATIONS COMMUNITY 1

Security Vendors' Analysis

BitDefender	Malware	CyRadar	Malicious
G-Data	Malware	Seclookup	Malicious
alphaMountain.ai	Suspicious	Abusix	Clean

In-Class Lab #7

1) Created a web application that will accept user input and store it in the backend DB



```
from flask import Flask, request, redirect
from flask.templating import render_template
from flask.sqlalchemy import SQLAlchemy
from flask_migrate import Migrate, migrate
import logging

logging.basicConfig(filename='record.log', level=logging.DEBUG, format=f'%(asctime)s %(levelname)s %(name)s %(threadName)s : %(message)s')

app = Flask(__name__)
app.debug = True

# adding configuration for using a sqlite database
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///site.db'

# Creating an SQLAlchemy instance
db = SQLAlchemy(app)

# Settings for migrations
migrate = Migrate(app, db)

# Models
class Profile(db.Model):
    # Id : Field which stores unique id for every row in
    # database table.
    # First names used to store the first name of the user.
```

At line:1 char:1
+ env\scripts\activate
+ ~~~~~
+ CategoryInfo : ObjectNotFound: (env\scripts\activate:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CouldNotAutoLoadModule

PS C:\Users\Fireb\Desktop\Coding Projects\Python Folder> cd "c:\Users\Fireb\Desktop\Coding Projects\Python Folder\.vscode\Lab_7_Forensics"
PS C:\Users\Fireb\Desktop\Coding Projects\Python Folder\.vscode\Lab_7_Forensics> env\scripts\activate
(env) PS C:\Users\Fireb\Desktop\Coding Projects\Python Folder\.vscode\Lab_7_Forensics> python -u "c:\Users\Fireb\Desktop\Coding Projects\Python Folder\.vscode\Lab_7_Forensics\app.py"
* Serving Flask app 'app'
* Debug mode: on
(env) PS C:\Users\Fireb\Desktop\Coding Projects\Python Folder\.vscode\Lab_7_Forensics>

← → ↺ ⓘ 127.0.0.1:5000

Profiles

ADD

Id First Name Last Name Age #

Profile form

First Name Last Name Age

Profiles

[ADD](#)

Id	First Name	Last Name	Age	#
1	Jackson	Yuan	28	Delete

2) Recorded HTTP server and DB logs my application creates

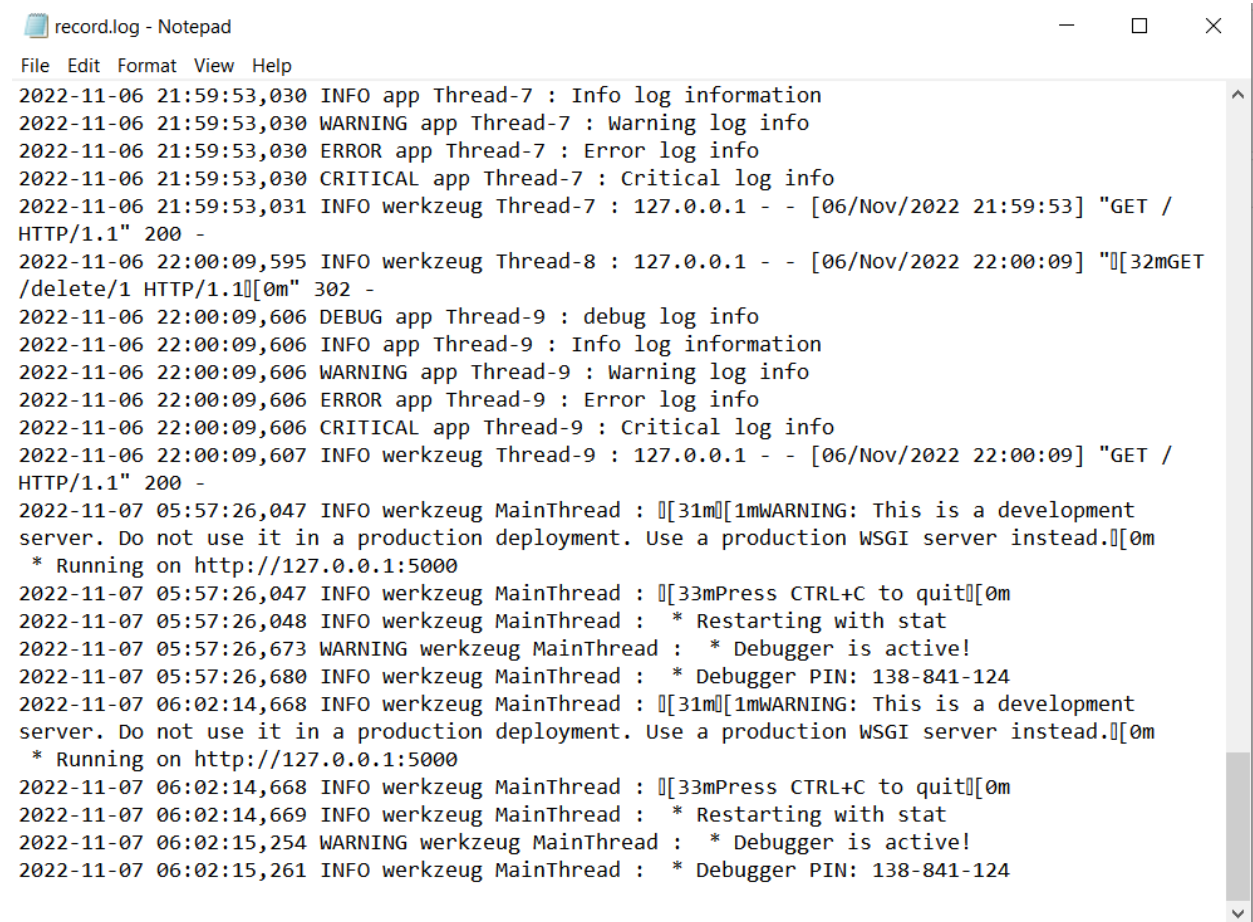
Running web application (picture below)

```
TERMINAL  PROBLEMS  51  OUTPUT
(env) PS C:\Users\fireb\Desktop
ab_7_Forensics\app.py"
* Serving Flask app 'app'
* Debug mode: on
```

Log file created (picture below)

Name	Date modified
__pycache__	11/4/2022 1:54 AM
env	10/26/2022 1:54 AM
instance	11/6/2022 10:00 PM
migrations	11/4/2022 12:34 AM
templates	11/4/2022 1:04 AM
app.py	11/7/2022 6:02 AM
record.log	11/7/2022 5:57 AM

Collection of information inside the log file (Picture below)



```
record.log - Notepad
File Edit Format View Help
2022-11-06 21:59:53,030 INFO app Thread-7 : Info log information
2022-11-06 21:59:53,030 WARNING app Thread-7 : Warning log info
2022-11-06 21:59:53,030 ERROR app Thread-7 : Error log info
2022-11-06 21:59:53,030 CRITICAL app Thread-7 : Critical log info
2022-11-06 21:59:53,031 INFO werkzeug Thread-7 : 127.0.0.1 - - [06/Nov/2022 21:59:53] "GET /
HTTP/1.1" 200 -
2022-11-06 22:00:09,595 INFO werkzeug Thread-8 : 127.0.0.1 - - [06/Nov/2022 22:00:09] "[32mGET
/delete/1 HTTP/1.1[0m" 302 -
2022-11-06 22:00:09,606 DEBUG app Thread-9 : debug log info
2022-11-06 22:00:09,606 INFO app Thread-9 : Info log information
2022-11-06 22:00:09,606 WARNING app Thread-9 : Warning log info
2022-11-06 22:00:09,606 ERROR app Thread-9 : Error log info
2022-11-06 22:00:09,606 CRITICAL app Thread-9 : Critical log info
2022-11-06 22:00:09,607 INFO werkzeug Thread-9 : 127.0.0.1 - - [06/Nov/2022 22:00:09] "GET /
HTTP/1.1" 200 -
2022-11-07 05:57:26,047 INFO werkzeug MainThread : [31m[1mWARNING: This is a development
server. Do not use it in a production deployment. Use a production WSGI server instead.[0m
* Running on http://127.0.0.1:5000
2022-11-07 05:57:26,047 INFO werkzeug MainThread : [33mPress CTRL+C to quit[0m
2022-11-07 05:57:26,048 INFO werkzeug MainThread : * Restarting with stat
2022-11-07 05:57:26,673 WARNING werkzeug MainThread : * Debugger is active!
2022-11-07 05:57:26,680 INFO werkzeug MainThread : * Debugger PIN: 138-841-124
2022-11-07 06:02:14,668 INFO werkzeug MainThread : [31m[1mWARNING: This is a development
server. Do not use it in a production deployment. Use a production WSGI server instead.[0m
* Running on http://127.0.0.1:5000
2022-11-07 06:02:14,668 INFO werkzeug MainThread : [33mPress CTRL+C to quit[0m
2022-11-07 06:02:14,669 INFO werkzeug MainThread : * Restarting with stat
2022-11-07 06:02:15,254 WARNING werkzeug MainThread : * Debugger is active!
2022-11-07 06:02:15,261 INFO werkzeug MainThread : * Debugger PIN: 138-841-124
```

3) Forward the logs to Splunk instance using splunk forwarder. During selection process, I picked the exact location of my log files on my host computer.

Forwarded inputs

Type	Inputs	Actions
Windows Event Logs Collect event logs from forwarders.	5	+ Add new
Files & Directories Monitor files or directories on forwarders.	1	+ Add new
Windows Performance Monitoring Collect performance data from forwarders.	0	+ Add new
TCP Configure a forwarder to listen on a TCP port for incoming data.	0	+ Add new
UDP Configure a forwarder to listen on a UDP port for incoming data.	0	+ Add new
Scripts Collect data from scripts installed on forwarders.	0	+ Add new

Files & directories

Data inputs > Files & directories

Showing 1-1 of 1 item

filter

25 per page

Source path	Host	Source type	Index	Server Class	Status	Actions
C:\Users\fireb\Desktop\Coding Projects\Python Folder\vscode\Lab_7_Forensics\record.log	None	Automatic	default	Domain Controller	Enabled Disable	Delete

4) Run a search in Splunk to show the application (web and DB) data forwarded from host pc.

New Search

source="C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log"

✓ 203 events (before 11/7/22 7:19:29.000 AM) No Event Sampling ▼

i	Time	Event
>	11/7/22 7:11:08.552 AM	2022-11-07 07:11:08,552 INFO werkzeug Thread-14 : 127.0.0.1 - - [07/Nov/2022 07:11:08] "GET / HTTP/1.1" 200 - host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:08.551 AM	2022-11-07 07:11:08,551 CRITICAL app Thread-14 : Critical log info host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:08.551 AM	2022-11-07 07:11:08,551 ERROR app Thread-14 : Error log info host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:08.551 AM	2022-11-07 07:11:08,551 WARNING app Thread-14 : Warning log info host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:08.551 AM	2022-11-07 07:11:08,551 INFO app Thread-14 : Info log information host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:08.551 AM	2022-11-07 07:11:08,551 DEBUG app Thread-14 : debug log info host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:08.540 AM	2022-11-07 07:11:08,540 INFO werkzeug Thread-13 : 127.0.0.1 - - [07/Nov/2022 07:11:08] " [32mPOST /add HTTP/1.1 [0m" 302 - host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:04.459 AM	2022-11-07 07:11:04,459 INFO werkzeug Thread-12 : 127.0.0.1 - - [07/Nov/2022 07:11:04] "GET /add_data HTTP/1.1" 200 - host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:02.013 AM	2022-11-07 07:11:02,013 INFO werkzeug Thread-11 : 127.0.0.1 - - [07/Nov/2022 07:11:02] "GET / HTTP/1.1" 200 - host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:11:02.013 AM	2022-11-07 07:11:02,013 CRITICAL app Thread-11 : Critical log info host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:10:43.691 AM	2022-11-07 07:10:43,691 INFO werkzeug MainThread : * Debugger PIN: 138-841-124 host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:10:43.685 AM	2022-11-07 07:10:43,685 WARNING werkzeug MainThread : * Debugger is active! host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:10:43.028 AM	2022-11-07 07:10:43,028 INFO werkzeug MainThread : * Restarting with stat host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:10:43.027 AM	2022-11-07 07:10:43,027 INFO werkzeug MainThread : [33mPress CTRL+C to quit [0m host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 7:10:43.027 AM	2022-11-07 07:10:43,027 INFO werkzeug MainThread : [31m [1mWARNING: This is a development server. Do not use it in a production WSGI server instead. [0m * Running on http://127.0.0.1:5000 host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22 6:15:45.085 AM	2022-11-07 06:15:45,085 INFO werkzeug Thread-12 : 127.0.0.1 - - [07/Nov/2022 06:15:45] "GET / HTTP/1.1" 200 - host = NEWNEW source = C:\\Users\\fireb\\Desktop\\Coding Projects\\Python Folder\\vscode\\Lab_7_Forensics\\record.log sourcetype = record
>	11/7/22	2022-11-07 06:15:45,084 CRITICAL app Thread-12 : Critical log info

User Name: fireb Password: 12345678