

Solving k3anu_evidence pcap with Zeek - Sean Yarkoni

Solving the challenge k3anu_evidence with Zeek on Ubuntu-20.04.2-live-server-amd64.

The challenges are:

- 1) What is the hostname of the system the PCAP was recovered from? (all caps)
- 2) What is the user agent K3anu use?
- 3) What operating system did K3anu use?
- 4) How many different DNS queries are in the PCAP file?
- 5) How many DNS queries in the PCAP received NXdomain?
- 6) What IP and port does the executable came from?
- 7) What is the name of the executable that was sent?
- 8) What can be find using different Zeek signature?

PCAP file working with can be found in:

<https://drive.google.com/file/d/1bimpl4aHw25n87On47fMqQQsTX168gna/view>

Solution:

In order for us to start we need Zeek to read the PCAP file. For that will need to type: `zeek -r k3anu_evidence.pcapng ->` This command will tell Zeek to read the file and create different Log files that Zeek can create using the information that can be found in the PCAP file.



Now we can start solving the challenge.

- 1) The hostname of the system the PCAP was recovered from can be found in the dhcp.log file because when a computer need to get an IP address it needs to identify itself in front of the DHCP server, we can see the hostname by typing: `less -S dhcp.log` and the hostname is: MSEDGEWIN10.

```
#open 2021-04-06-13-28-47
#fields ts uid5 client_addr server_addr mac host_name client_fqdn domain requested_addr assigned_addr lease time client_message server_message
#types time set[string] addr addr string string string string interval string vector[string] interval
1512946400.107601 C75ndZ3zRw39I4Xoqa,CpG52U3gsmxU908014 10.0.2.15 10.0.2.2 08:00:27:f8:91:8f MSEDGEWIN10 MSEDGEWIN10 - 10.0.2.15 10.0.2.15
#close 2021-04-06-13-28-48
```

2) The user agent K3anu using can be found in the http.log file under the user agent column and we can find it by using the IP address found in challenge 1 from the dhcp.log file IP-10.0.2.15 by typing: less -S http.log we can see that the user agent is: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36 .

ts	uid	id.orig.h	id.orig.p	id.resp.h	id.resp.p	trans_depth	method	host	uri	referrer	version	user_agent	origin	request_body_len	response_body_len	status_code	status_msg	
Fileds	time	string	addr	port	addr	port	count	string	string	string	string	count	count	string	string	string	vector[string]	vector[string]
1512945820	185492		Gdaul1P3l3hKjuka	10.0.2.15	49920	104.16.91.188	80	1	GET	crt.comodoca.com	/C/COODORSAA8TrustCA.crt	-	1.1	Microsoft-CryptoAPI/10.0	-	0	1480	200 OK
1512945820	185492		Cv9wR1lmePdcv3	10.0.2.15	49921	104.16.91.188	80	1	GET	crt.comodoca.com	/C/COODORSAA8TrustCA.crt	-	1.1	Microsoft-CryptoAPI/10.0	-	0	1480	200 OK
1512945820	122614		C5u6M2hvj3zz7rda	10.0.2.15	49922	23.73.142.145	80	1	GET	ssl.trustwusa.com	/issuers/STCA.crt	-	1.1	Microsoft-CryptoAPI/10.0	-	0	956	200 OK
1512945845	631884		Cj30X0Z000oufeVke	10.0.2.15	50223	50.63.243.228	80	1	GET	certificates.godaddy.com	/repository/gdigi2.crt	-	1.1	Microsoft-CryptoAPI/10.0	-	0	1236	200 OK
1512945849	563787		CEVv7M4gJc550Auhx	10.0.2.15	50248	74.121.138.36	80	1	GET	sync.mathing.com	/sync/imp/et_xid=68redir=http://sync.optimatic.com/4.5/web/service/cc.ssh/advertiser_id=medil_nsp0003AuisDP1501	-	1.1	AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36	-	-	-	
1512945849	579401		C1u2oemC8Vjyldet	10.0.2.15	50249	104.156.222.130	80	1	GET	x.bidmitch.net	/sync?app=optimatic	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945849	635044		CFvXV3E5Hw4sJ16	10.0.2.15	50250	50.18.186.105	80	1	GET	match.adsrvr.org	/track/cf/generic?ttid=pid=optimatic&ttid=tpid=	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945871	896998		CH9qC38jtmWzupkb	10.0.2.15	50464	34.228.34.48	80	1	GET	ncim-global.dsp.io	/pix? -	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945871	896931		COE8H7m7F4S0L30	10.0.2.15	50467	23.13.228.237	80	1	GET	tags.bluekai.com	/site/436876?id=3084-02-18278597-0	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	676305		ChwPv2h0w0g27L3	10.0.2.15	50501	45.33.49.119	80	1	GET	seclists.org	/shared/css/insecdb.css	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	186201		ChwS0AL7e5S0LXL8	10.0.2.15	50506	172.217.12.98	80	1	GET	pagead2.googlesyndication.com	/pagead/js/adsbygoogle.js	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	156697		CSC6M1q2Mx5S8R1g	10.0.2.15	50502	45.33.49.119	80	1	GET	seclists.org	/images/ritelogo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	242783		CH9q4tq2Vj3Zy6d	10.0.2.15	50505	45.33.49.119	80	1	GET	seclists.org	/shared/images/legitflow.gif	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	244311		CH9T8v0M1ZVys9e	10.0.2.15	50504	45.33.49.119	80	1	GET	seclists.org	/images/maw-maw-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	244600		Chw1D1ZM4u060	10.0.2.15	50503	45.33.49.119	80	1	GET	seclists.org	/images/current-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	165205		ChwPv2h0w0g27L3	10.0.2.15	50501	45.33.49.119	80	2	GET	seclists.org	/shared/images/Accounting-asa-Check-40.gif	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	506081		ChwPv2h0w0g27L3	10.0.2.15	50505	45.33.49.119	80	1	GET	seclists.org	/shared/images/Accounting-asa-Check-40.gif	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	
1512945900	363085		CSC6M1q2Mx5S8R1g	10.0.2.15	50502	45.33.49.119	80	2	GET	seclists.org	/images/archive-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	-	-	-	

3) The operating system K3anu use can be seen in the user agent we found in challenge 2 (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36) and the operating system is: Windows NT 10.0; Win64; x64.

4) The amount of the DNS queries that are in the PCAP file can be found by using Zeek-cut on the dns.log file and by organizing the results, we need to type: less -S dns.log | /usr/local/zeek/bin/zeek-cut query | sort -u | wc -l and then we can see that 860 queries were made in the PCAP file.

```
eliot@kali:~/Desktop/k3anu_evidence$ less -S dns.log | /usr/local/zeek/bin/zeek-cut query | sort -u | wc -l
860
```

5) We can find how many DNS queries NXdomain received in the PCAP file by looking at the file dns.log and grepping NXdomain, we will type: less -S dns.log | grep -iE nxdomain and see that there are 5 DNS queries in the PCAP file to NXdomain

eliot@kali:~/Desktop/k3anu_evidence\$ less -S dns.log grep -iE nxdomain																	
1512946223.036412			CHLW92n0G0wEUGK1	10.0.2.15	58617	10.0.2.3	53	udp	19272	-	a.collective-media.net	1	C	INTERNET	1	A	3
1512946242.165975			CmAGaQ3ESNRjFzK431	10.0.2.15	52726	10.0.2.3	53	udp	50405	-	ad.mydomain.com	1	C	INTERNET	1	A	3
1512946247.421014			Cgajzq2sBVr2Zg2yG3	10.0.2.15	53204	10.0.2.3	53	udp	45168	-	ad.mydomain.com	1	C	INTERNET	1	A	3
1512947864.194148			COaG453Dy1Xjri0ej4	10.0.2.15	51888	10.0.2.3	53	udp	27494	-	t.tellapart.com	1	C	INTERNET	1	A	3
1512948243.561470			Coz1HB2ufz8T8WmZt1	10.0.2.15	63761	10.0.2.3	53	udp	25081	-	t.tellapart.com	1	C	INTERNET	1	A	3

6) The IP and port the executable came from can be found by looking at the pe.log file that contain portable executable information by typing: less -S pe.log we can see that Zeek found only 1 executable in the PCAP file, we can grep the id string Zeek gave to that portable executable and find more information on the file by typing: grep F1cWhZUGFS6Zf11Zd *.log , now we can see that the file came from 104.131.112.255 on port 21

eliot@kali:~/Desktop/k3anu_evidence\$ grep F1cWhZUGFS6Zf11Zd *.log															
Fileds	log	1512947346.413816	F1cWhZUGFS6Zf11Zd	104.131.112.255	10.0.2.15	Cv7RjBeu9Xk20VURS	FTP_DATA	0	PE	application/x-dosexec	-	0.389970	-	F	485
ec	log	1512947346.373753	CCZ8zr59P9GevKh7	10.0.2.15	52786	104.131.112.255 21	plggy	<hidden>	RETR	ftp://104.131.112.255/home/plggy/decrypttool.exe	application/x-dosexec	-	-	-	-
ec	log	4859786.226	Transfer complete.												
ec	log	1512947358.082365	CCZ8zr59P9GevKh7	10.0.2.15	52786	104.131.112.255 21	plggy	<hidden>	PASV	-	-	227	Entering Passive Mode (104,131,112,255,214,		
ec	log	1512947346.414750	F1cWhZUGFS6Zf11Zd	104.131.112.255	10.0.2.15	54855	plggy	<hidden>	RETR	ftp://104.131.112.255/home/plggy/decrypttool.exe	application/x-dosexec	-	-	-	-
text	data	data	data	data	data	data	data	data	data	data	data	data	data	data	data

7) The name of the executable that was sent can be found using what we found in the previous challenge (challenge 6) and if we type: grep F1cWhZUGFS6Zf11Zd *.log we can see that there is a file sent from 104.131.112.255/home/plggy and its called decrypttool.exe which is the executable we were trying to find and as we know from the pe.log it is the only executable in the PCAP file.

http host	referrer	version	agent	origin	request body_len	response body_len	status code	status msg	info code	info msg	user-agent
string	count	count	string	set[enum]	string	string set[string]	vector[string]	vector[string]	vector[string]	vector[string]	vector[string]
crt.comodoca.com	/C/MOD08SAADTrustCA.crt	-	1.1	Microsoft-CryptAPI/10.0	-	0	1400	200 OK	-	(empty)	-
crt.comodoca.com	/C/MOD08SAADTrustCA.crt	-	1.1	Microsoft-CryptAPI/10.0	-	0	1400	200 OK	-	(empty)	-
ssl.trustwave.com	/Issuers/STICA.crt	-	1.1	Microsoft-CryptAPI/10.0	-	0	956	200 OK	-	(empty)	-
certificate.caddy.com	/api/v1/certificates/gspig.crt	-	1.1	Microsoft-CryptAPI/10.0	-	0	1256	200 OK	-	(empty)	-
sync.mathatg.net	/sync/img?mt=0x4c68&redir=/sync/optimatic.com/v4.5/wbservice/cc.ashx?advertiser_id=medid.5d0001GUID=PM.UUID)	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
x.bidsixnet.net	/sync/sync-optimatic	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
match.adsrvr.org	/track/cm/?generic?ttid=paid-optimatic&tclid=1	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
eicm.com	/wp-content/uploads/2017/06/1684-02-19276597-6	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
test.bluesky.com	/css/images/6x6-1684-02-19276597-6	-	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/shared/css/insecure.css	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
pagead2.googlesyndication.com	/pagead/js/adsbygoogle.js	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/site/logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/shared/images/icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/mmap-dev-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/current-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/shared/images/Acutnic/xch Chess-MB.gif	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/archive-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/archive-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
pagead2.googlesyndication.com	/pagead/js/r20171129/r20171010/show_ads_impl.js	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/feed-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/about-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/minus-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/plus-icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/fulldisclosure-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/map-announce-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/basgo-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/hugtraq-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/pen-test-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/focus-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/icon-16x16.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/first-aid-kit-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/webappsec-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0
seclists.org	/images/pauldotco-logo.png	http://seclists.org/	1.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36	-	0	0	0	0	0	0

If we want to get more organized information we can go to the ".sig" file we created at the start of this challenge and type:

Sudo vim <name>.sig

And in the file:

signature <name> {

```
ip-proto == tcp
```

dst-port == 80

```
http-request //
```

```
http-request-header //
```

event "<name>"

}

Now we can go back to the PCAP file and read it with Zeek and add the signature file and type:

```
zeek -r k3anu_evidence.pcapng -s /home/eliot/zeek/scripts/base/protocols/test/test.sig
```

Now we can go to the new file created signatures.log and see that the file contains only connections on port 80 but with the same data as the http.log file.

```

10.0.2.15: Found accountname! GET /COMODORSAAadTrustCa.crt HTTP/1.1x8dVxbAConnection: Keep-Alivex8dVxbAccept: */*x8dVxbUser-Agent: Microsoft-CryptAPI/10.0(x8dVxbHost: crt
10.0.2.15: Found accountname! GET /COMODORSAAdTrustCa.crt HTTP/1.1x8dVxbAConnection: Keep-Alivex8dVxbAccept: */*x8dVxbUser-Agent: Microsoft-CryptAPI/10.0(x8dVxbHost: crt
10.0.2.15: Found accountname! GET /issuers/STCA.crt HTTP/1.1x8dVxbAConnection: Keep-Alivex8dVxbAccept: */*x8dVxbUser-Agent: Microsoft-CryptAPI/10.0(x8dVxbHost: ssl.trustw
10.0.2.15: Found accountname! GET /repository/gidc.crt HTTP/1.1x8dVxbAConnection: Keep-Alivex8dVxbAccept: */*x8dVxbUser-Agent: Microsoft-CryptAPI/10.0(x8dVxbHost: certifi
10.0.2.15: Found accountname! GET /api/v1/metrics/redir/http://192.168.1.7:80?metric=system.cpu.usage HTTP/1.1x8dVxbHost: x.bioswitch.netx8dVxbAConnection: keep-alivex8dVxbUser-Age
10.0.2.15: Found accountname! GET /sync.asp?optimatic=http://1.x8dVxbAHost: x.bioswitch.netx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; WinIn
name! 10.0.2.15 has triggered signature my- on 5 hosts - 5
GET /track/cm/generic/tst pid=optimatic/stdt tpi=1 HTTP/1.1x8dVxbAHost: match.adsrvr.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/
10.0.2.15: Found accountname! GET /pix? HTTP/1.1x8dVxbAHost: eicm-global.dsp.iox8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
10.0.2.15: Found accountname! GET/site/43696f6e1684-b2-192769f5-6 HTTP/1.1x8dVxbHost: taps.bluelink.comx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows
10.0.2.15: Found accountname! GET /HTTP/1.1x8dVxbAHost: seclists.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
10.0.2.15: Found accountname! GET /shared/css/insecdb.css HTTP/1.1x8dVxbHost: seclists.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
10.0.2.15: Found accountname! GET /images/site/logo.png HTTP/1.1x8dVxbHost: seclists.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET /pages/fedback/google.js HTTP/1.1x8dVxbHost: pagead2.googleysyndication.comx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Win
name! 10.0.2.15 has triggered signature my- on 10 hosts - 10
GET /shared/images/topleftcurve.gif HTTP/1.1x8dVxbAHost: seclists.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win
10.0.2.15: Found accountname! GET /images/nmap-dev-logo.png HTTP/1.1x8dVxbAHost: seclists.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win
10.0.2.15: Found accountname! GET /images/current-icon-lbx16.jpg HTTP/1.1x8dVxbAHost: seclists.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win
10.0.2.15: Found accountname! GET /adsense/search/asynv-adcs.js HTTP/1.1x8dVxbAHost: cse.google.comx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0
10.0.2.15: Found accountname! GET /generate_204 HTTP/1.1x8dVxbAHost: client1.google.comx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET / HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUpgrade-Insecure-Requests: 1x8dVxbUser-Agent: Mozilla/5.0 (Windows N
10.0.2.15: Found accountname! GET /shares/images/Acutemix/acx_chess-MB.gif HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windo
10.0.2.15: Found accountname! GET /logos/wireshare-88x344.png HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Wi
10.0.2.15: Found accountname! GET /flags/home-icon.png HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET /flags/wiki-icon.png HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET /generate_204 HTTP/1.1x8dVxbAHost: client1.google.comx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET /shared/images/tiny-eyeicon.png HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET /tap/linux/H/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUpgrade-Insecure-Requests: 1x8dVxbUser-Agent: Mozilla/5.0 (Wind
10.0.2.15: Found accountname! GET /logos/webscarab-B0x87.png HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Wl
10.0.2.15: Found accountname! GET /generate_204 HTTP/1.1x8dVxbAHost: client1.google.comx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET /tools/tcpdump.html HTTP/1.1x8dVxbAHost: sectools.orgx8dVxbAConnection: keep-alivex8dVxbUpgrade-Insecure-Requests: 1x8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
10.0.2.15: Found accountname! GET / HTTP/1.1x8dVxbAHost: secwiki.orgx8dVxbAConnection: keep-alivex8dVxbUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x

```

Ssl.log is a file containing SSL/TLS handshake info.

Weird.log is a file containing session initiation protocol.

x509.log is a file containing X.509 certificate info.

3) We saw that the log files Zeek generate show us rich related information that can be found in each packet wan Zeek read the pcap file with his "out of the box" settings, each file is sorted in a way that it is easy to read and understand in order for us to find what we need easily.

4) We saw that Zeek give's packets a string that we can copy and grep to find related information connected to the packet from different log files and it will be easier to us to "dig" through a suspicions or interesting connection.

5) We experience with Zeek a very versatile signatures that we can make in order to get the information we are after, but in order to get that signature right and the information relevant, we need to know in which protocol and layer the information we want to get is supposed to be, when using signature, the user knowledge have a big role.