



ELABORATO CORSO RETI DI CALCOLATORI: RACCOLTA E ANALISI DI TRACCE DI TRAFFICO DI APPLICAZIONI VIDEO MOBILI

A.A. 2019/2020

Docente: Antonio Pescapè

Gruppo: gruppo_rdc_3

Componenti: Claudio Russo (N46003988), Benito Visone (N46003959).

PROCEDURA SPERIMENTALE EFFETTUATA

Per la cattura delle tracce di traffico sono stati utilizzati due dispositivi:

- **Huawei P-Smart 2019** (Android 10)
- **Huawei P-20 lite** (Android 9)

Le applicazioni utilizzate sono state le seguenti:

- **tPacketCapture**: Allo scopo di catturare le tracce di traffico.
- **Termux**: Utilizzato per eseguire lo script 'mobile_traceroute.sh' che restituisce i risultati relativi alla traccia in ingresso:
 - ➔ Nslookup
 - ➔ Elenco servizi contattati (Protocollo di trasporto ed indirizzo)
 - ➔ Traceroute di ogni indirizzo contattato

Sono state effettuate complessivamente 8 catture, 4 per ogni dispositivo utilizzato. In particolare, per ogni dispositivo sono state effettuate 2 catture su Rete 4G e 2 catture su Rete WiFi.

Ciascuna cattura ha una durata di circa 30 minuti ed è relativa all'applicazione **Vimeo** (com.vimeo.android.videoapp) , in particolare è stato analizzato il traffico relativo alla riproduzione del seguente contenuto: <https://vimeo.com/70718629>.

Prima di ogni cattura sono stati revocati i permessi di accesso alla rete Internet di ciascuna applicazione installata sul dispositivo fatta eccezione per l'applicazione oggetto di analisi (Vimeo) e l'applicazione tPacketCapture.

Immediatamente dopo ciascuna cattura, sono stati riassegnati i permessi di accesso alla rete all'applicazione Termux al fine di eseguire lo script 'mobile_traceroute.sh'.

Successivamente i risultati grezzi dello script sono stati trasferiti su notebook per l'analisi.

L'analisi è stata effettuata utilizzando il sottosistema Ubuntu presente su Windows, in particolare utilizzando i seguenti strumenti:

- **tshark**
- **capinfos**

Le procedure di analisi sono state automatizzate mediante uno script realizzato in linguaggio Python 3 (fornito in allegato).

I comandi utilizzati per la realizzazione dell'analisi sono i seguenti:

- **Estrazione informazioni generali sulla traccia catturata mediante capinfos:**

```
capinfos -TmQ *.pcap >gruppo_rdc_3.csv
```

Tale comando fornisce informazioni sintetiche di interesse su ciascuna cattura.

- **Estrazione dei biflussi TCP/UDP mediante tshark:**

```
tshark -r cattura.pcap -qz conv,tcp > tcp_conversations.txt  
tshark -r cattura.pcap -qz conv,udp > udp_conversations.txt
```

Tale comando restituisce, per ogni cattura, l'elenco dei biflussi analizzati. Ogni biflusso è una quintupla formata da: indirizzo IP sorgente, Numero di porta sorgente, indirizzo IP destinazione, Numero di porta destinazione, protocollo a livello di trasporto. Inoltre, per ogni biflusso, il comando restituisce il numero di byte e di frame relativi sia al flusso in upstream che in downstream. È inoltre fornito il totale di tali valori.

- **Risoluzione DNS mediante tshark con filtro sul campo dns.flag.response:**

```
tshark -r cattura.pcap -T fields -E separator=, -E quote=d -e frame.time_epoch -e ip.src -e ip.dst -e  
ip.proto -e tcp.srcport -e tcp.dstport -e dns.a -e dns.qry.name -Y "(dns.flags.response == 1  
)">cattura.csv
```

Tale comando restituisce l'insieme dei campi definito dal parametro -e. Inoltre effettua un filtro sui pacchetti analizzati, restituendo esclusivamente i pacchetti relativi a risposte DNS.

- **Estrazione campo SNI di TLS mediante tshark:**

```
tshark -r cattura.pcap -T fields -E separator=, -E quote=d -e frame.time_epoch -e ip.src -e ip.dst -e  
ip.proto -e tcp.srcport -e tcp.dstport -e tls.handshake.extensions_server_name -E  
header=y,separator=/t -Y "ssl.handshake.extensions_server_name" >sni_extraction.csv
```

Tale comando restituisce l'insieme dei campi definito dal parametro -e. Inoltre effettua un filtro sui pacchetti analizzati, restituendo esclusivamente i pacchetti che contengono un valore per il campo SNI, relativo al protocollo TLS.

- **Estrazione campo Host di http mediante tshark:**

```
tshark -r cattura.pcap -T fields -E separator=, -E quote=d -e frame.time_epoch -e ip.src -e ip.dst -e  
ip.proto -e tcp.srcport -e tcp.dstport -e http.host -E header=y,separator=/t -Y 'http'  
>http_extraction.csv
```

Tale comando restituisce l'insieme dei campi definito dal parametro -e. Inoltre effettua un filtro sui pacchetti analizzati, restituendo esclusivamente i pacchetti che contengono un valore per il campo HOST, relativo al protocollo http.

DESCRIZIONE FUNZIONAMENTO SCRIPT

Per l'elaborazione delle tracce di traffico è stato realizzato uno script Python al fine di ottenere una coppia di file riportanti le informazioni complessive relative ai biflussi (TCP/UDP) estratti.

Lo script prende in ingresso le tracce di traffico e per ciascuna di esse restituisce due file *tcp_conversations.txt* e *udp_conversations.txt* contenenti rispettivamente i biflussi TCP ed UDP estratti. A questo punto lo script effettua una fase di pretrattamento dei dati convertendo i file .txt in file .csv, facilmente elaborabili mediante l'utilizzo di un foglio di calcolo (e.g. Excel).

Successivamente vengono estratte per ogni cattura le informazioni relative ai campi DNS, SNI (TLS), HOST (http) e tali informazioni vengono memorizzate in tre file separati:

sni_extraction.csv, http_extraction.csv, dns_extraction.csv.

La fase finale consiste nel confrontare separatamente i biflussi presenti nei file *tcp_conversations.csv*, *udp_conversations.csv* con le informazioni contenute nei file *sni_extraction.csv*, *http_extraction.csv*, *dns_extraction.csv* al fine di ottenere due file riportanti le informazioni complessive relative ai biflussi estratti:

tcp_conversations_result.csv, udp_conversations_result.csv.

TRACCE ANALIZZATE - *N.B. Alcune informazioni sono state nascoste per motivi di impaginazione ma sono presenti nei documenti allegati.*

- Traccia 1: russo_4g1.pcap
Dispositivo: Huawei P-20 lite (Android 9)
Operatore mobile: Vodafone

Risultato ricavato dal tool capinfos

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
russo_4g1.pcap	us	65535	25579	161246693	160837405	1800.109123	22/06/2020 18:53	22/06/2020 19:23	89348.70	714789.58	6287.87	14.21

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_IP	SRC_PO RT	DST_IP	DST_PO RT	LEFT_FRAM ES	LEFT_BYT ES	RIGHT_FRAM ES	RIGHT_BYT ES	SNI	DNS	HTT P
10.8.0.1	47054	84.53.177.49	443	5166	76356135	5166	443183	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	47108	84.53.177.49	443	1570	21878116	1570	141611	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	33512	216.58.209.42	443	516	186809	517	157125	N\D	N\D	N\D
10.8.0.1	55300	66.102.1.188	5228	42	8340	41	3988	N\D	N\D	N\D
10.8.0.1	54358	151.101.192.7	443	30	46579	32	11906	N\D	N\D	N\D
10.8.0.1	42974	52.44.106.171	443	24	2939	27	7687	analytics.localytics.com	N\D	N\D
10.8.0.1	52958	52.71.187.57	443	20	7233	21	4644	N\D	N\D	N\D
10.8.0.1	60560	52.3.44.9	443	19	6849	19	3000	profile.localytics.com	N\D	N\D
10.8.0.1	47854	216.58.208.18	443	15	3510	17	3611	N\D	N\D	N\D
10.8.0.1	54500	151.101.192.2 17	443	13	1666	15	2356	N\D	N\D	N\D
10.8.0.1	60926	143.204.11.42	443	11	1537	12	2477	api.branch.io	N\D	N\D
10.8.0.1	45214	35.168.179.19	443	10	854	11	1507	N\D	N\D	N\D
10.8.0.1	33086	216.58.198.42	443	8	2574	9	2211	android.googleapis.com	N\D	N\D
10.8.0.1	57668	34.253.3.138	443	6	5435	6	662	telemetry.api.swiftkey.com	N\D	N\D
10.8.0.1	52484	216.58.208.12	443	4	216	5	475	N\D	N\D	N\D
10.8.0.1	35270	216.58.206.74	443	4	216	5	807	firebaseremoteconfig.googleapi s.com	N\D	N\D

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	47989	216.58.198.36	443	37	26720	39	14493	N\D	N\D	N\D

- Traccia 2: russo_4g2.pcap
Dispositivo: Huawei P-20 lite (Android 9)
Operatore mobile: Vodafone

Risultato ricavato dal tool capinfos

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
russo_4g2.pcap	us	65535	15093	160756864	160515352	1802.009354	22/06/2020 20:28	22/06/2020 20:58	89075.76	712606.08	10635.09	8.38

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	38528	151.101.242.109	443	2358	70601959	2352	211865	skyfire.vimeocdn.com	N\D	N\D
10.8.0.1	38516	151.101.242.109	443	816	21499643	815	70668	N\D	N\D	N\D
10.8.0.1	33882	216.58.209.42	443	644	224190	645	188894	N\D	N\D	N\D
10.8.0.1	46982	172.217.21.74	443	146	52226	148	43869	N\D	N\D	N\D
10.8.0.1	52292	216.58.206.42	443	35	79605	37	14065	www.googleapis.com	N\D	N\D
10.8.0.1	42668	151.101.128.217	443	28	5087	30	10888	api.vimeo.com	N\D	N\D
10.8.0.1	55634	34.195.212.200	443	25	8108	26	6661	profile.localytics.com	N\D	N\D
10.8.0.1	43332	52.44.106.171	443	16	6657	18	3040	N\D	N\D	N\D
10.8.0.1	52626	52.23.134.99	443	14	6909	14	4262	N\D	N\D	N\D
10.8.0.1	36872	143.204.11.52	443	12	6402	13	2242	N\D	N\D	N\D
10.8.0.1	52304	216.58.206.42	443	11	1938	13	2358	firebaseremoteconfig.googleapis.com	N\D	N\D
10.8.0.1	48040	216.58.208.138	443	11	5262	12	2030	N\D	N\D	N\D
10.8.0.1	55782	34.195.212.200	443	12	6471	11	2543	profile.localytics.com	N\D	N\D
10.8.0.1	46028	143.204.11.20	443	11	6073	11	1165	N\D	N\D	N\D
10.8.0.1	37032	143.204.11.52	443	7	947	8	1892	api.branch.io	N\D	N\D
10.8.0.1	45570	216.58.198.36	443	6	536	7	1042	N\D	N\D	N\D
10.8.0.1	42640	151.101.128.217	443	4	216	5	468	api.vimeo.com	N\D	N\D
10.8.0.1	40992	151.101.240.217	443	4	216	5	472	N\D	N\D	N\D
10.8.0.1	55222	151.101.64.217	443	4	216	5	807	api.vimeo.com	N\D	N\D

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	45206	216.58.198.36	443	31	28298	33	10071	N\D	N\D	N\D

- Traccia 3: russo_wifi1.pcap
Dispositivo: Huawei P-20 lite (Android 9)
Operatore Internet: Infostrada

Risultato ricavato dal tool capinfos

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
russo_wifi1.pcap	us	65535	9482	164332346	164180610	1952.537699	22/06/2020 14:17	22/06/2020 14:50	84085.76	672686.05	17314.98	4.86

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_I P	SRC_PO RT	DST_IP	DST_PO RT	LEFT_FRA MES	LEFT_BYT ES	RIGHT_FRA MES	RIGHT_BY TES	SNI	DN S	HTTP
10.8.0 .1	33890	216.58.206.7	443	274	96862	275	80769	firebase-remoteconfig.googleapis.com	N\	N\
10.8.0 .1	60110	216.58.209.4	443	121	12645	123	65215	N\	D	N\
10.8.0 .1	48576	216.58.198.4	443	108	6305034	111	7052	N\	D	N\
10.8.0 .1	48678	216.58.198.4	443	107	6268580	110	6999	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	45984	216.58.208.1	443	92	5312570	95	6187	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	46050	216.58.208.1	443	91	5248276	94	6134	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	48582	216.58.198.4	443	91	5252476	94	6134	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	48626	216.58.198.4	443	91	5248276	94	6134	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	48650	216.58.198.4	443	91	5245476	94	6135	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	48666	216.58.198.4	443	91	5239876	94	6135	N\	D	N\
10.8.0 .1	48734	216.58.198.4	443	91	5234276	94	6135	N\	D	N\
10.8.0 .1	48744	216.58.198.4	443	90	5186782	93	6081	N\	D	N\
10.8.0 .1	46020	216.58.208.1	443	75	4197172	78	5270	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	48740	216.58.198.4	443	75	4216772	78	5271	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	48564	216.58.198.4	443	74	4160878	77	5216	N\	D	N\
10.8.0 .1	48598	216.58.198.4	443	74	4144078	77	5216	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	48754	216.58.198.4	443	74	4344258	75	5078	N\	D	N\
10.8.0 .1	48552	216.58.198.4	443	58	3130774	61	4352	video-prod-skyfire-std-us.storage.googleapis.com	N\	N\
10.8.0 .1	40898	216.58.208.1	443	38	16800	40	10251	app-measurement.com	N\	N\
10.8.0 .1	45334	172.217.21.7	443	33	9947	35	13934	www.googleapis.com	N\	N\
10.8.0 .1	57860	34.227.164.1	443	32	9085	33	10850	analytics.localytics.com	N\	N\
10.8.0 .1	50020	216.58.205.7	443	29	10868	30	13639	N\	D	N\
10.8.0 .1	45338	172.217.21.7	443	26	5894	28	9824	N\	D	N\
10.8.0 .1	42128	80.158.36.56	5223	23	1644	25	1935	N\	D	N\
10.8.0 .1	46482	151.5.18.35	443	20	10997	21	2920	N\	D	N\
10.8.0 .1	46682	216.58.208.1	443	17	3598	19	3719	N\	D	N\
10.8.0 .1	59442	3.121.198.67	443	17	18628	18	4242	sodium.slp.pos.here.com	N\	N\

10.8.0		216.58.205.7							N\	
.1	49378	4	443	17	5064	16	2487	N\D	D	N\D
10.8.0								30vod-	N\	
.1	38662	151.5.18.19	443	15	37186	17	2718	adaptive.akamaized.net	D	N\D
10.8.0		216.58.198.1							N\	
.1	34578	0	443	13	2903	15	3166	N\D	D	N\D
10.8.0		151.29.122.3							N\	
.1	40358	2	443	13	2751	14	2557	N\D	D	N\D
10.8.0		216.58.209.4							N\	
.1	60096	2	443	12	4992	14	3460	play.googleapis.com	D	N\D
10.8.0		216.58.206.7						firebaseremoteconfig.googlea	N\	
.1	33762	4	443	13	5304	13	2084	pis.com	D	N\D
10.8.0		216.58.205.7							N\	
.1	49976	4	443	12	2163	14	2412	N\D	D	N\D
10.8.0		143.204.11.6							N\	
.1	57920	3	443	12	6402	13	2241	N\D	D	N\D
10.8.0									N\	
.1	42810	20.44.78.251	443	11	6243	14	1956	N\D	D	N\D
10.8.0		216.58.208.1						vimeo-prod-skyfire-std-	N\	
.1	45950	44	443	11	5288	12	1421	us.storage.googleapis.com	D	N\D
10.8.0		157.240.193.							N\	
.1	39830	18	443	10	1822	12	1624	graph.facebook.com	D	N\D
10.8.0		157.240.193.							N\	
.1	39906	18	443	10	1368	11	2147	N\D	D	N\D
10.8.0		151.29.122.3							N\	
.1	50218	3	443	10	2092	11	1809	N\D	D	N\D
10.8.0		216.58.208.1						vimeo-prod-skyfire-std-	N\	
.1	45976	44	443	10	17502	11	1651	us.storage.googleapis.com	D	N\D
10.8.0		151.101.114.							N\	
.1	52854	109	443	9	45218	12	1199	i.vimeocdn.com	D	N\D
10.8.0		216.58.208.1							N\	
.1	40446	74	443	9	5452	11	1459	N\D	D	N\D
10.8.0		151.29.122.3						30vod-	N\	
.1	50212	3	443	9	35300	11	1809	adaptive.akamaized.net	D	N\D
10.8.0		151.29.122.3							N\	
.1	50250	3	443	9	35266	11	1809	N\D	D	N\D
10.8.0		151.29.122.3						30vod-	N\	
.1	40382	2	443	9	638	10	1754	adaptive.akamaized.net	D	N\D
10.8.0		216.58.208.1							N\	
.1	46000	44	443	9	2048	10	1598	N\D	D	N\D
10.8.0		216.58.208.1							N\	
.1	46008	44	443	9	2048	10	1598	N\D	D	N\D
10.8.0		216.58.208.1							N\	
.1	46016	44	443	9	2048	10	1598	N\D	D	N\D
10.8.0		216.58.208.1							N\	
.1	46086	44	443	9	2048	10	1598	N\D	D	N\D
10.8.0		216.58.208.1						vimeo-prod-skyfire-std-	N\	
.1	46098	44	443	9	2048	10	1598	us.storage.googleapis.com	D	N\D
10.8.0		216.58.198.4						vimeo-prod-skyfire-std-	N\	
.1	48606	8	443	9	2048	10	1598	us.storage.googleapis.com	D	N\D
10.8.0		216.58.198.4							N\	
.1	48622	8	443	9	2048	10	1598	N\D	D	N\D
10.8.0		216.58.198.4						vimeo-prod-skyfire-std-	N\	
.1	48634	8	443	9	2048	10	1598	us.storage.googleapis.com	D	N\D
10.8.0		216.58.206.3							N\	
.1	45738	3	443	8	6269	10	1269	N\D	D	N\D
10.8.0		216.58.206.3							N\	
.1	45742	3	443	7	6215	9	1215	lh5.googleusercontent.com	D	N\D
10.8.0									N\	
.1	37436	143.204.11.8	443	7	947	8	1891	N\D	D	N\D
10.8.0									N\	radiomap.vcdn.pos.her
.1	42090	2.21.164.48	80	7	1195	7	680	N\D	D	e.com
10.8.0		52.232.222.1							N\	
.1	38866	05	443	4	216	5	471	N\D	D	N\D
10.8.0		172.217.21.7							N\	
.1	45222	4	443	4	216	5	807	N\D	D	N\D
10.8.0		52.232.216.8							N\	
.1	51124	6	443	4	216	5	471	N\D	D	N\D
10.8.0		151.29.122.3							N\	
.1	50258	3	443	4	216	5	807	N\D	D	N\D
10.8.0		216.58.198.1							N\	
.1	34792	0	443	4	216	5	807	N\D	D	N\D
10.8.0		192.168.1.25							N\	
.1	42146	4	7	3	162	4	236	N\D	D	N\D
10.8.0		157.240.193.							N\	
.1	39708	18	443	2	108	4	256	N\D	D	N\D
10.8.0		157.240.193.							N\	
.1	39688	18	443	1	54	2	128	N\D	D	N\D
10.8.0		5.249.149.11							N\	
.1	60418	2	80	1	54	2	128	N\D	D	N\D

10.8.0	99.86.162.19									N\
.1	51606	7	443	1	54	2	128	N\	D	N\

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	45785	216.58.206.33	443	70	86263	71	7937	N\	N\	N\
10.8.0.1	40835	216.58.206.33	443	1	1392	2	1513	N\	N\	N\

- Traccia 4: russo_wifi2.pcap
Dispositivo: Huawei P-20 lite (Android 9)
Operatore Internet: Infostrada

Risultato ricavato dal tool capinfos

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
russo_wifi2.pcap	us	65535	19225	173733873	173426249	1845.471810	22/06/2020 15:09	22/06/2020 15:40	93973.94	751791.48	9020.87	10.42

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	41022	151.29.122.32	443	2707	76132786	2711	270246	N\	N\	N\
10.8.0.1	47410	151.5.18.35	443	1164	37563297	1165	111743	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	47216	216.58.208.138	443	616	219243	617	184271	N\	N\	N\
10.8.0.1	41026	151.29.122.32	443	417	8685673	418	49030	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	60590	216.58.198.42	443	162	56243	164	47844	firebaseconfig.googleapis.com	N\	N\
10.8.0.1	41098	151.29.122.32	443	100	3645594	101	12135	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	41130	151.29.122.32	443	84	2688043	85	11250	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	58420	64.233.166.188	5228	83	37265	71	5835	mtalk.google.com	N\	N\
10.8.0.1	58598	34.227.164.12	443	36	9564	36	11774	analytics.localytics.com	N\	N\
10.8.0.1	59746	52.3.44.9	443	27	8185	26	6665	N\	N\	N\
10.8.0.1	32926	216.58.209.42	443	25	6338	27	9697	N\	N\	N\
10.8.0.1	50882	151.29.122.33	443	18	10933	19	2814	N\	N\	N\
10.8.0.1	51146	216.58.208.170	443	17	5272	19	3728	play.googleapis.com	N\	N\
10.8.0.1	39402	151.5.18.19	443	14	4107	15	2621	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	51078	216.58.208.170	443	14	3520	15	3503	N\	N\	N\
10.8.0.1	42874	34.225.218.211	443	14	6909	14	4244	analytics.localytics.com	N\	N\
10.8.0.1	45762	40.70.152.245	443	13	6320	14	1956	N\	N\	N\
10.8.0.1	50886	151.29.122.33	443	12	37001	14	2397	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	41096	151.29.122.32	443	11	746	14	2029	N\	N\	N\
10.8.0.1	51086	216.58.208.170	443	11	2057	13	2358	N\	N\	N\
10.8.0.1	41178	151.29.122.32	443	11	23997	13	1923	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	60518	216.58.198.42	443	11	5045	12	2030	firebaseconfig.googleapis.com	N\	N\
10.8.0.1	41146	151.29.122.32	443	11	21116	12	1891	30vod-adaptive.akamaized.net	N\	N\
10.8.0.1	45552	52.1.140.196	443	11	6134	11	1550	N\	N\	N\

10.8.0.1	40974	151.29.122.32	443	10	2092	11	1814	N\D	N\D	N\D
10.8.0.1	40998	151.29.122.32	443	10	2092	11	1814	N\D	N\D	N\D
10.8.0.1	51490	143.204.11.121	443	10	6019	10	1111	N\D	N\D	N\D
10.8.0.1	41138	151.29.122.32	443	9	23831	11	1815	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	51070	151.29.122.33	443	9	638	10	1783	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	37744	151.101.242.109	443	8	21704	11	1145	N\D	N\D	N\D
10.8.0.1	51066	151.29.122.33	443	8	23701	9	1707	N\D	N\D	N\D
10.8.0.1	54180	151.101.64.217	443	4	216	5	468	api.vimeo.com	N\D	N\D
10.8.0.1	50966	151.29.122.33	443	4	216	5	807	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	51074	151.29.122.33	443	4	216	5	807	N\D	N\D	N\D
10.8.0.1	52232	151.101.0.217	443	2	108	3	699	N\D	N\D	N\D

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

- Traccia 5: visone_4g1.pcap
Dispositivo: Huawei P-Smart 2019 (Android 10)
Operatore Internet: WindTre

Risultato ricavato dal tool capinfos

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
visone_4g1.pcap	us	65535	54355	163629254	162759550	1814.270511	21/06/2020 10:59	21/06/2020 11:29	89710.74	717685.92	2994.38	29.96

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	36588	151.29.122.32	443	10977	67189608	10975	748680	N\D	N\D	N\D
10.8.0.1	45190	151.5.24.32	443	3889	21110570	3890	258496	N\D	N\D	N\D
10.8.0.1	43188	216.58.198.10	443	339	112844	340	95697	firebaseremoteconfig.googleapis.com	N\D	N\D
10.8.0.1	48588	151.5.24.18	443	109	332128	110	8979	N\D	N\D	N\D
10.8.0.1	33726	151.101.128.217	443	69	10833	52	14072	api.vimeo.com	N\D	N\D
10.8.0.1	53508	172.217.21.74	443	44	14830	45	12291	firebaseremoteconfig.googleapis.com	N\D	N\D
10.8.0.1	47202	80.158.45.93	5223	29	2073	30	2323	N\D	N\D	N\D
10.8.0.1	38630	52.44.78.190	443	20	7129	19	3621	profile.localytics.com	N\D	N\D
10.8.0.1	35398	52.0.195.163	443	18	6734	18	4185	N\D	N\D	N\D
10.8.0.1	52188	80.158.2.190	6447	16	4684	17	3313	N\D	N\D	N\D
10.8.0.1	48910	52.86.79.224	443	14	6518	14	2982	analytics.localytics.com	N\D	N\D
10.8.0.1	42436	143.204.11.37	443	13	6181	14	2098	N\D	N\D	N\D
10.8.0.1	33780	151.101.128.217	443	12	2477	13	3015	N\D	N\D	N\D

10.8.0.1	48908	52.86.79.224	443	12	6313	12	1584	N\D	N\D	N\D
10.8.0.1	39548	80.158.20.104	443	11	5096	12	1740	N\D	N\D	N\D
10.8.0.1	51756	34.206.101.182	443	11	6134	11	1524	N\D	N\D	N\D
10.173.122.222	42746	216.58.205.74	443	10	2635	11	2279	firebaseremoteconfig.googleapis.com	N\D	N\D
10.8.0.1	42172	151.101.240.217	443	10	7016	11	1660	player.vimeo.com	N\D	N\D
10.8.0.1	33758	216.58.205.74	443	5	270	6	923	firebaseremoteconfig.googleapis.com	N\D	N\D
10.8.0.1	56212	157.240.193.35	443	5	560	5	1475	b-graph.facebook.com	N\D	N\D
10.8.0.1	37796	151.29.122.33	443	4	216	5	807	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	53428	157.240.193.18	443	3	452	3	573	api.facebook.com	N\D	N\D
10.8.0.1	53432	157.240.193.18	443	3	452	3	575	graph.facebook.com	N\D	N\D

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	60799	157.240.193.18	443	1	1294	2	2548	N\D	N\D	N\D
10.8.0.1	55609	151.5.216.130	53	1	161	1	98	N\D	N\D	N\D
10.8.0.1	56190	151.5.216.130	53	1	147	1	87	N\D	N\D	N\D

- Traccia 6: visone_4g2.pcap
Dispositivo: Huawei P-Smart 2019 (Android 10)
Operatore Internet: WindTre

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
visone_4g2.pcap	us	65535	53555	172281395	171424491	1895.370129	21/06/2020 14:00	21/06/2020 14:31	90443.81	723550.46	3200.91	28.26

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	49442	151.5.18.35	443	5423	35612155	5421	355865	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	49668	151.5.18.35	443	3309	23669909	3310	216478	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	41292	151.21.209.4	443	2062	13060716	2063	153273	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	52108	216.58.208.170	443	1625	564109	1626	467567	firebaseremoteconfig.googleapis.com	N\D	N\D
10.8.0.1	49590	151.5.18.35	443	1146	8398803	1147	75774	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	41264	151.21.209.4	443	255	1792877	254	16749	N\D	N\D	N\D
10.8.0.1	41272	151.21.209.4	443	191	1000549	192	13999	N\D	N\D	N\D
10.8.0.1	41240	151.21.209.4	443	113	801935	112	7885	N\D	N\D	N\D
10.8.0.1	41256	151.21.209.4	443	66	246598	66	5401	N\D	N\D	N\D
10.8.0.1	41210	151.21.209.4	443	61	331582	60	5055	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	49648	151.5.18.35	443	55	337962	56	4263	N\D	N\D	N\D
10.8.0.1	39620	74.125.206.188	5228	44	8152	42	3886	mtalk.google.com	N\D	N\D
10.8.0.1	52112	216.58.208.170	443	36	11666	37	9839	N\D	N\D	N\D
10.8.0.1	41214	151.21.209.4	443	32	373524	31	3532	N\D	N\D	N\D
10.8.0.1	33832	216.58.208.138	443	27	7043	29	6341	firebaseremoteconfig.googleapis.com	N\D	N\D

10.8.0									N\	
.1	47320	31.13.86.49	5222	27	2440	27	2638	N\D	D	N\D
10.8.0		151.101.0.21							N\	
.1	47146	7	443	23	8553	24	8336	api.vimeo.com	D	N\D
10.8.0		151.21.209.4							N\	
.1	41248	1	443	23	149142	22	2427	N\D	D	N\D
10.8.0									N\	
.1	56768	31.13.86.49	443	20	1961	19	1524	N\D	D	N\D
10.8.0		216.58.206.4						firebase-remoteconfig.googleapis.com	N\	
.1	37758	2	443	17	4225	19	3757		D	N\D
10.8.0		151.21.209.4							N\	
.1	41228	1	443	18	140404	17	2156	30vod-adaptive.akamaized.net	D	N\D
10.8.0		151.21.209.4							N\	
.1	41284	1	443	16	133132	17	2135	30vod-adaptive.akamaized.net	D	N\D
10.8.0									N\	
.1	56970	31.13.86.49	443	16	2088	16	1791	N\D	D	N\D
10.8.0		152.195.132.						configdownload-dre.dbankcdn.com	N\	
.1	37226	192	443	14	12127	17	2715		D	N\D
10.8.0		52.72.203.21							N\	
.1	41072	2	443	15	6572	15	4602	N\D	D	N\D
10.8.0									N\	
.1	56742	31.13.86.49	443	15	1737	13	1089	N\D	D	N\D
10.8.0									N\	
.1	51346	52.1.140.196	443	13	6242	13	1632	manifest.localytics.com	D	N\D
10.8.0									N\	
.1	41974	31.13.86.8	443	12	5050	13	1677	graph.facebook.com	D	N\D
10.8.0		52.204.205.7							N\	
.1	41386	6	443	12	6313	12	1584	N\D	D	N\D
10.8.0		151.101.240.							N\	
.1	46804	217	443	10	7016	11	1660	N\D	D	N\D
10.8.0		80.158.20.10							N\	
.1	43986	4	443	9	5019	11	1686	N\D	D	N\D
10.8.0		151.101.240.							N\	
.1	47018	217	443	9	1827	10	1563	player.vimeo.com	D	N\D
10.8.0		157.240.193.							N\	
.1	57998	18	443	7	385	8	989	N\D	D	N\D
10.8.0		157.240.193.							N\	
.1	58002	18	443	7	385	8	989	graph.facebook.com	D	N\D
10.8.0		151.101.0.21							N\	
.1	47636	7	443	7	1342	8	1978	N\D	D	N\D
10.8.0									N\	
.1	55514	52.71.170.14	443	5	270	7	606	profile.localytics.com	D	N\D
10.8.0									N\	
.1	58400	35.174.142.0	443	5	270	7	608	N\D	D	N\D
10.8.0									N\	
.1	36454	143.204.11.8	443	5	270	7	935	N\D	D	N\D
10.8.0		157.240.193.							N\	
.1	57966	18	443	6	2628	5	956	api.facebook.com	D	N\D
10.8.0									N\	
.1	60406	151.5.18.19	443	4	216	5	807	30vod-adaptive.akamaized.net	D	N\D
10.8.0		157.240.193.							N\	
.1	57974	18	443	1	54	1	74	N\D	D	N\D
10.8.0		157.240.193.							N\	
.1	60756	35	443	1	54	1	74	N\D	D	N\D
10.8.0		157.240.193.							N\	
.1	57982	18	443	1	54	1	74	N\D	D	N\D

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	45206	216.58.198.36	443	31	28298	33	10071	N\D	N\D	N\D

- Traccia 7: visone_wifi1.pcap
Dispositivo: Huawei P-Smart 2019 (Android 10)
Operatore Internet: Linkem S.p.A.

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
visone_wifi1.pcap	us	65535	51271	179879130	179058770	1804.940966	21/06/2020 11:54	21/06/2020 12:24	99204.78	793638.23	3492.40	28.41

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_PACKETS	LEFT_BYTES	RIGHT_PACKETS	RIGHT_BYTES	SNI	DN	HTT
10.8.0.1	37978	2.16.135.104	443	8041	61424457	8042	564704	N\	D	N\
10.8.0.1	34810	185.5.63.77	443	2499	12972413	2500	136523	N\	D	N\
10.8.0.1	34266	216.58.206.4	443	989	319168	990	267745	firebaseremoteconfig.googleapis.com	N\	D
10.8.0.1	38696	2.16.135.104	443	778	3704126	779	53305	30vod-adaptive.akamaized.net	N\	D
10.8.0.1	38780	2.16.135.104	443	440	2524341	441	30892	30vod-adaptive.akamaized.net	N\	D
10.8.0.1	57914	2.16.135.138	443	355	1366498	356	24381	30vod-adaptive.akamaized.net	N\	D
10.8.0.1	57938	2.16.135.138	443	192	992641	193	17540	N\	D	N\
10.8.0.1	34344	216.58.206.4	443	127	43946	129	37291	N\	D	N\
10.8.0.1	43906	151.101.0.21	443	77	11487	59	17204	api.vimeo.com	N\	D
10.8.0.1	37808	185.5.63.162	443	40	214019	39	3094	N\	D	N\
10.8.0.1	43962	151.101.0.21	443	34	8515	35	13277	N\	D	N\
10.8.0.1	51340	34.193.38.11	443	33	3634	31	2757	N\	D	N\
10.8.0.1	35826	157.240.193.55	443	28	2882	28	2153	N\	D	N\
10.8.0.1	45428	157.240.193.55	5222	27	2733	27	2105	N\	D	N\
10.8.0.1	55248	35.174.142.0	443	27	7642	25	8835	analytics.localytics.com	N\	D
10.8.0.1	48642	80.158.45.93	5223	25	1787	26	2037	N\	D	N\
10.8.0.1	33490	157.240.11.5	5222	24	1989	25	1982	N\	D	N\
10.8.0.1	35652	157.240.193.55	443	23	2974	22	1793	N\	D	N\
10.8.0.1	43982	151.101.0.21	443	19	49743	20	4872	api.vimeo.com	N\	D
10.8.0.1	44620	216.58.198.1	443	19	5045	18	2314	N\	D	N\
10.8.0.1	35456	157.240.193.55	443	18	2789	16	1616	N\	D	N\
10.8.0.1	53918	157.240.193.50	443	16	22535	16	1798	N\	D	N\
10.8.0.1	56378	52.73.1.96	443	15	6963	14	4226	analytics.localytics.com	N\	D
10.8.0.1	54846	157.240.193.18	443	12	5050	16	1887	N\	D	N\
10.8.0.1	59778	52.232.216.8	443	12	6266	13	2236	N\	D	N\
10.8.0.1	56744	173.194.160.200	443	12	6766	13	2127	r2---sn-hpa7zn76.gvt1.com	N\	D
10.8.0.1	49536	54.192.73.8	443	12	6127	12	1558	cdn.branch.io	N\	D
10.8.0.1	43640	151.101.240.217	443	11	7070	12	1714	N\	D	N\
10.8.0.1	48066	52.1.140.196	443	11	6134	11	1524	manifest.localytics.com	N\	D

10.8.0	157.240.193.								N\	
.1	54838	18	443	10	4943	11	1569	N\D	D	N\D
10.8.0									N\	
.1	49390	54.192.73.12	443	9	5866	10	2074	N\D	D	N\D
10.8.0	157.240.193.								N\	
.1	57658	35	443	6	638	5	1475	b-graph.facebook.com	D	N\D
10.8.0									N\	
.1	59676	54.192.73.3	443	4	216	5	807	cdn.branch.io	D	N\D
10.8.0	151.101.0.21								N\	
.1	43958	7	443	4	216	5	807	api.vimeo.com	D	N\D
10.8.0									N\	
.1	58038	2.16.135.138	443	4	216	5	807	30vod-adaptive.akamaized.net	D	N\D
10.8.0	173.194.160.								N\	
.1	56674	200	443	4	216	5	807	r2---sn-hpa7zn76.gvt1.com	D	N\D
10.8.0	157.240.193.								N\	
.1	54874	18	443	4	2496	3	404	api.facebook.com	D	N\D
10.8.0	151.101.192.								N\	
.1	60678	217	443	2	108	3	699	api.vimeo.com	D	N\D

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	60767	157.240.193.18	443	1	1294	2	2548	N\D	N\D	N\D
10.8.0.1	33739	216.239.35.4	123	1	90	1	90	N\D	N\D	N\D
10.8.0.1	45139	192.168.1.1	53	1	145	1	98	N\D	N\D	N\D
10.8.0.1	38803	192.168.1.1	53	1	147	1	87	N\D	N\D	N\D

- Traccia 8: visone_wifi2.pcap
Dispositivo: Huawei P-Smart 2019 (Android 10)
Operatore Internet: Linkem S.p.A.

File name	File time precision	Packet size limit	Number of packets	File size (bytes)	Data size (bytes)	Capture duration (seconds)	Start time	End time	Data byte rate (bytes/sec)	Data bit rate (bits/sec)	Average packet size (bytes)	Average packet rate (packets/sec)
visone_wifi2.pcap	us	65535	38706	150414225	149794905	1636.550862	21/06/2020 13:14	21/06/2020 13:41	91530.86	732246.87	3870.07	23.65

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi TCP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	39916	2.16.135.104	443	10873	100710471	10874	763770	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	60524	2.16.135.138	443	1927	9499042	1928	142148	30vod-adaptive.akamaized.net	N\D	N\D
10.8.0.1	39926	2.16.135.104	443	894	7903457	896	77758	N\D	N\D	N\D
10.8.0.1	40284	2.16.135.104	443	224	1418860	226	15239	N\D	N\D	N\D
10.8.0.1	33386	151.101.192.217	443	86	58920	69	14534	api.vimeo.com	N\D	N\D
10.8.0.1	33448	151.101.192.217	443	33	46864	34	8265	api.vimeo.com	N\D	N\D
10.8.0.1	37288	52.2.87.203	443	31	9031	33	11074	N\D	N\D	N\D
10.8.0.1	37388	157.240.193.55	443	27	2542	27	2468	N\D	N\D	N\D
10.8.0.1	35134	52.97.168.210	993	24	6979	19	1994	outlook.office365.com	N\D	N\D
10.8.0.1	46740	157.240.193.55	5222	19	3234	17	1762	N\D	N\D	N\D
10.8.0.1	53956	13.224.13.124	443	13	6456	14	2634	api.branch.io	N\D	N\D

10.8.0.1	33468	151.101.192.217	443	12	2050	13	3021	api.vimeo.com	N\D	N\D
10.8.0.1	46244	216.58.206.74	443	11	2504	13	2411	N\D	N\D	N\D
10.8.0.1	45886	151.101.240.217	443	11	7088	12	1714	N\D	N\D	N\D
10.8.0.1	50430	35.173.209.179	443	11	6134	11	1524	N\D	N\D	N\D
10.8.0.1	46354	216.58.198.10	443	10	5313	11	2241	N\D	N\D	N\D
10.8.0.1	39746	99.86.33.112	443	10	6019	10	1450	cdn.branch.io	N\D	N\D
10.8.0.1	57128	157.240.193.18	443	7	668	6	1633	graph.facebook.com	N\D	N\D
10.8.0.1	45862	151.101.240.217	443	4	216	5	807	N\D	N\D	N\D
10.8.0.1	36804	216.58.206.78	80	4	299	4	418	N\D	N\D	clients3.google.com
10.8.0.1	59900	157.240.193.35	443	4	506	3	575	N\D	N\D	N\D

Risultato ricavato dal tool tshark e script Python: Analisi Biflussi UDP

SRC_IP	SRC_PORT	DST_IP	DST_PORT	LEFT_FRAMES	LEFT_BYTES	RIGHT_FRAMES	RIGHT_BYTES	SNI	DNS	HTTP
10.8.0.1	56885	157.240.193.18	443	1	1294	2	2548	N\D	N\D	N\D

CONSIDERAZIONI:

Una prima considerazione riguarda la differenza nel **numero di pacchetti** e **relative dimensioni** tra le tracce di traffico catturate su rete 4G e su rete WiFi. In particolare, come si evince dalle informazioni riportate dal tool capinfos, le catture effettuate su rete 4G presentano un numero maggiore di pacchetti rispetto alle catture effettuate su rete WiFi, aventi però dimensioni minori.

Come ci aspettavamo, la maggior parte del traffico è costituito da segmenti **TCP** che risultano preponderanti rispetto ai segmenti **UDP** in quanto le applicazioni di Streaming Video utilizzano principalmente **TCP** come protocollo a livello di trasporto, anche se in realtà lo Streaming Video può tollerare una certa perdita di pacchetti.

Abbiamo riscontrato dei problemi nel *matching* tra gli indirizzi IP Destinazione e i risultati ottenuti attraverso le risoluzioni **DNS**. Inoltre, ci aspettavamo un numero maggiore di pacchetti relativi a richieste **DNS**, in relazione all'elevato numero di indirizzi IP Destinazione rilevati dall'analisi dei Biflussi.

Essendo i campi SNI ed HOST (http) mutuamente esclusivi, dall'analisi effettuata si evince che la maggior parte del traffico fa uso di un protocollo di comunicazione criptato. Effettuando un confronto con i documenti fornitici dalla traccia dell'elaborato, in particolare [wei2012profiledroid] dal quale si evince che **in precedenza la maggior parte del traffico di rete era non criptato**, i risultati ottenuti dimostrano come la rete si stia spostando negli anni sempre più verso un tipo di comunicazione sicura. Ovviamente tale considerazione è frutto solo della nostra esperienza con l'applicazione Vimeo.

Tra i vari Host contattati, rientrano Host facente riferimento a Vimeo, come ad esempio:

- *fire.vimeocdn.com*
- *api.vimeo.com*
- *player.vimeo.com*

Host che rappresentano tipici esempi di CDN tra cui:

- *cdn.branch.io*
- *30vod-adaptive.akamaized.net*
- *configdownload-dre.dbankcdn.com*
- *i.vimeocdn.com*

Host che non sembrano essere legati a servizi di CDN, la maggior parte dei quali facente riferimento a Google, tra cui:

- *clients3.google.com*
- *firebase-remoteconfig.googleapis.com*
- *mtalk.google.com*
- *eo-prod-skyfire-std-us.storage.googleapis.com*
- *lh5.googleusercontent.com*
- *play.googleapis.com*
- *www.googleapis.com*
- *android.googleapis.com*

Host facente riferimento ad altre aziende, come ad esempio:

- *graph.facebook.com*
- *api.facebook.com*
- *analytics.localytics.com*
- *manifest.localytics.com*

In riferimento a quanto riportato in [seneviratne2015short] circa il 60 % delle applicazioni a pagamento è connessa a dei **tracker** che memorizzano informazioni personali sull'utilizzo della rete, mentre nelle applicazioni gratuite questa percentuale si attesta intorno al 95%. Di conseguenza possiamo giustificare l'elevato numero di Host di natura differente che compaiono nelle catture in base al fatto che abbiamo utilizzato l'applicazione Vimeo nella sua versione gratuita. In particolare, tra i tracker individuato citiamo:

- Google Analytics - www.google.com/analytics/
- Localytics - www.localytics.com