

Caso Práctico: Fundamentos de Seguridad Cloud e Infraestructuras Industriales.

Desarrollo de Caso.

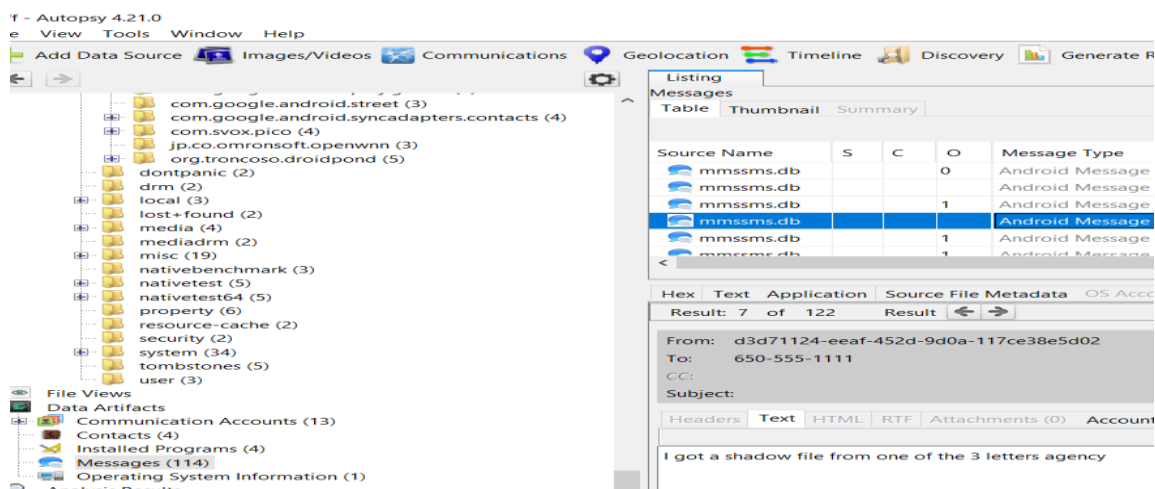
Análisis Forense de Dispositivos Móviles.

Hemos confiscado el celular de un sospechoso llamado Mr X, hemos volcado los datos del mismo (fichero adjunto a esta práctica) y necesitamos que se analicen y nos puedan ayudar con las siguientes preguntas principales (detallarlas, explicar y demostrar cómo se han conseguido):

- ¿Qué tramaba Mr X?

Ocupa ayuda para desencriptar el archivo SHADOW el cual contiene los hashes de usuarios y claves en sistemas operativos Linux. Este archivo aparentemente pertenecía al personal de un organismo norteamericano.

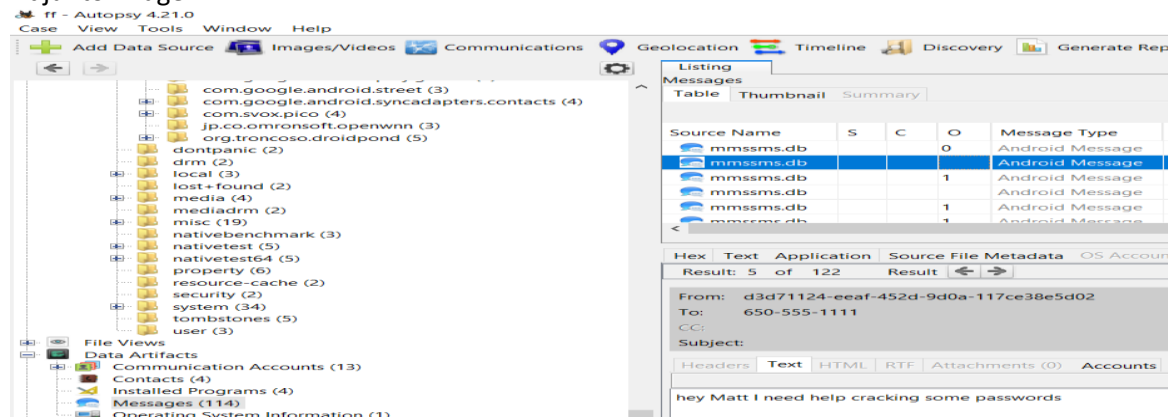
Adjunto imagen de la conversación utilizando el programa Autopsy.



- ¿A quién le pidió ayuda inicialmente?

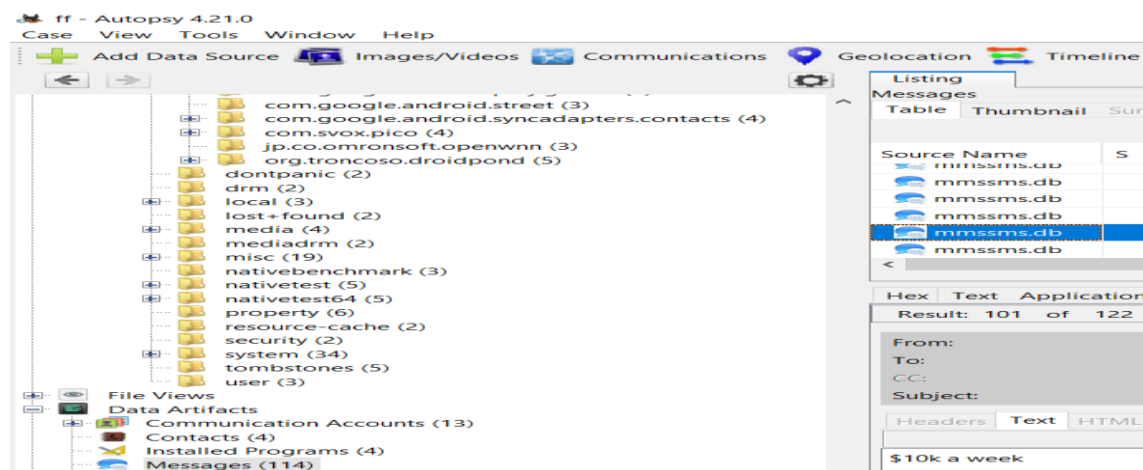
A Matt Murdock.

Adjunto imagen.



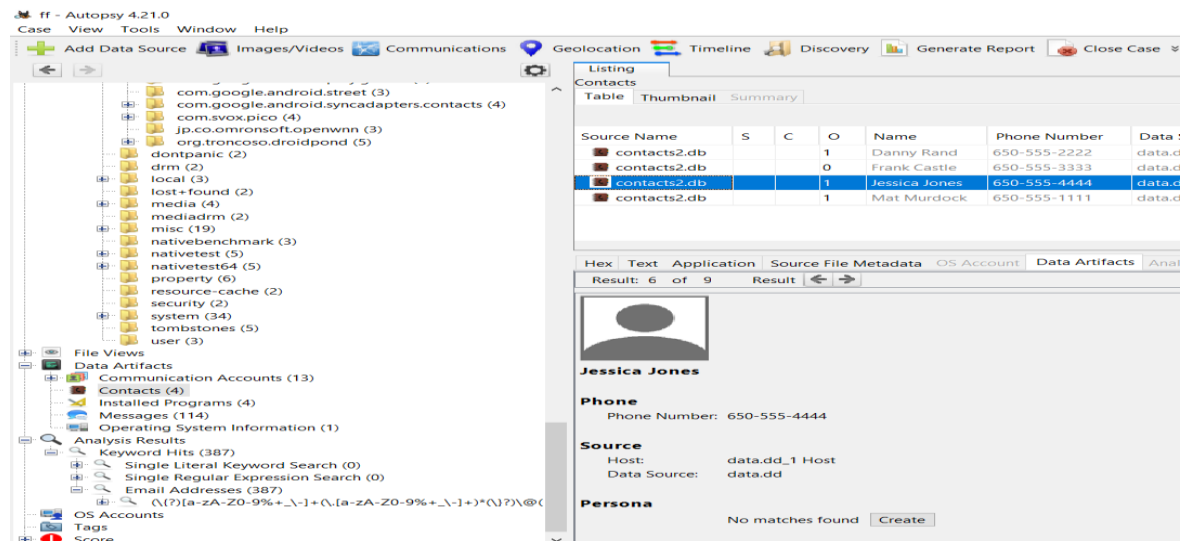
- ¿Quién le intentó ayudar? ¿Por cuánto dinero?

Danny Rand por \$10000 por semana.



• ¿Quién le paso el enlace del fichero a Mr X?

Jessica Jones.



• ¿Cuál es dicho enlace?

<https://cyberhades.ams3.digitaloceanspaces.com/shadow>

Además, también se solicita para resolver el caso:

- **El historial del navegador, incluyendo cookies si es posible**

```

1 Bookmarks 1 0 0 1 1 google_chrome_bookmarks
2 Google http://www.google.com/ 0 1 0 0 1 1483195917911 0
3 Picasa http://picasaweb.google.com/ 0 1 2 0 1 1483195917911 0
4 Yahoo! http://www.yahoo.com/ 0 1 4 0 1 1483195917911 0
5 MSN http://www.msn.com/ 0 1 6 0 1 1483195917911 0
6 Twitter http://twitter.com/ 0 1 8 0 1 1483195917911 0
7 Facebook http://www.facebook.com/ 0 1 10 0 1 1483195917911 0
8 Wikipedia http://www.wikipedia.org/ 0 1 12 0 1 1483195917911 0
9 eBay http://www.ebay.com/ 0 1 14 0 1 1483195917911 0
10 CNN http://www.cnn.com/ 0 1 16 0 1 1483195917911 0
11 NY Times http://www.nytimes.com/ 0 1 18 0 1 1483195917911 0
12 ESPN http://espn.com/ 0 1 20 0 1 1483195917911 0
13 Amazon http://www.amazon.com/ 0 1 22 0 1 1483195917911 0
14 Weather Channel http://www.weather.com/ 0 1 24 0 1 1483195917911 0
15 BBC http://www.bbc.co.uk/ 0 1 26 0 1 1483195917911 0

16 10 Most Popular Password Cracking Tools [Updated for 2018]
https://resources.infosecinstitute.com/10-popular-password-cracking-tools/ 0 1 -
9223372036854775808 0 1 1557395432504

```

Agrego COOKIES encontradas.

```

creation_utc host_key name value path expires_utc secure httponly last_access_utc
has_expires persistent priority encrypted_value
13201839896116275 .youtube.com YSC x6EshgWpZQk / 0 0 1 13201869057889038 0 0 1
13201839896116324 .youtube.com VISITOR_INFO1_LIVE mLqH884jW60 /
13217391896116324 0 1 13201869057889038 1 1 1
13201839899046445 .quantserve.com mc 5cd3861a-33b88-3b7b0-82262 /
13236054299046445 0 0 13201869076617658 1 1 1
13201839901854306 .cdn.viglink.com __cfduid
d6a79d34f47c321166efbc7bcd3daac931557366301 / 13233375901854306 0 1
13201869055762787 1 1 1
13201839902347132 links.services.disqus.com vglnk.Agent.p
995f3f99dc40d294a89b7b6675a66f88 / 13233375902347132 0 0 13201869056308317 1 1 1

```

13201839902347342 links.services.disqus.com vglInk.PartnerRfsh.p "" /
13233375902347342 0 0 13201869056308317 1 1 1
13201839903296970 .pippio.com did __l10oGFRXeoelTk / 13233375903296970 0 0
13201869057071679 1 1 1
13201839903297069 .pippio.com didts 1557366302 / 13233375903297069 0 0
13201869057071679 1 1 1
13201839903297167 .pippio.com nnls / 13207023903297167 0 0 13201869057071679 1
1 1
13201839903439742 .adsymptotic.com __cfduid
d2f72ac44137a9a36b54da62ef49b74901557366302 / 13233375903439742 0 1
13201869057617692 1 1 1
13201839903813888 .cogocast.net gpl 1| |t=1557366303 / 13201920000813888 0 0
13201839903813888 1 1 1
13201839903894189 .demdex.net demdex 54180333414598747682273490027540816408
/ 13217391903894189 0 0 13201839903894189 1 1 1
13201839903894262 .dpm.demdex.net dpm
54180333414598747682273490027540816408 / 13217391903894262 0 0 13201839903894262 1
1 1
13201839904181208 .mathtag.com uuid c2a05cd3-7de7-4e00-86bd-d44dd1db56bd /
13235795104181208 0 0 13201869057569150 1 1 1
13201839904193951 .cogocast.net dc_id
df7bf4dcea804595a826968c7690cf63| |t=1557366303 / 13264905601193951 0 0
13201839904193951 1 1 1
13201839904217154 .mathtag.com uuidc
z8GNk3xZfXdQcayELdWzLKUK3H58Dzi7vNttIOHIE5AaqU5YuCgvjJjMv5kWZrP9WKiw+LntbWtON1La
4vWMOYhHrMV2oPU4X/NT5tkfNiE= / 13235795104217154 0 0 13201869057569150 1 1 1
13201839904217611 .apxl.com dc_id
df7bf4dcea804595a826968c7690cf63| |t=1557366302 / 13285468801217611 0 0
13201839904217611 1 1 1
13201839930415074 search.supplyframe.com JSESSIONID
AAC0CF66B16345E905AA9D00BCEDC750.worker1 / 0 0 0 13201869045681576 0 0 1
13201839931536325 ads.supplyframe.com sfctx 413 / 13517372731536325 0 0
13201869045476103 1 1 1
13201839931915769 .prfct.co pa_mrin_ts 1557366331109 / 13264911931000000 0 0
13201869047358321 1 1 1
13201839931956995 .prfct.co pa_twitter_ts 1557366331156 / 13264911931000000 0 0
13201869047358321 1 1 1
13201839931957707 .prfct.co pa_crosswise_ts 1557366331157 / 13264911931000000 0 0
13201869047358321 1 1 1
13201839931981269 .prfct.co pa_yahoo_ts 1557366331185 / 13264911931000000 0 0
13201869047358321 1 1 1
13201839931981725 .prfct.co pa_openx_ts 1557366331187 / 13264911931000000 0 0
13201869047358321 1 1 1
13201839931983356 .facebook.com fr 0wk8jqy04BKxcRxHq..Bc04Y7...1.0.Bc04Y7. /
13209615931983356 1 1 13201869056304130 1 1 1
13201839931986072 .prfct.co pa_rubicon_ts 1557366331194 / 13264911931000000 0 0
13201869047358321 1 1 1

13201839932279331 .prfct.co pa_google_ts 1557366331466 / 13264911931000000 0 0
13201869047358321 1 1 1
13201839932298640 .twitter.com personalization_id "v1_cyZwsPSBbxwc5ZHKKJUX8A==" /
13264911932298640 0 0 13201868956014383 1 1 1
13201839932310971 pixel.rubiconproject.com c 1 / 0 0 0 13201869079523691 0 0 1
13201839932364546 .rubiconproject.com put_4106 pa_jVhQdpyJWcS1yhrXo /
13204259132364546 0 0 13201869078518614 1 1 1
13201839932735495 .nr-data.net JSESSIONID c74693c2f5c62ac4 / 0 1 0
13201839932735495 0 0 1
13201839933789519 .hackaday.com _fbp fb.1.1557366332191.594863907 /
13209615933000000 0 0 13201869044640152 1 1 1
13201839933792742 hackaday.com hd_cookie_notification_accepted true /
13233375933000000 0 0 13201869044640152 1 1 1
13201839975440921 .google.com CGIC
lkp0ZXh0L2h0bWwsYXBwbGljYXRpb24veGh0bWwreG1sLGFWcGxpY2F0aW9uL3htbDtxPTAuOSxpb
WFNzS93ZWJwLmCovKjtxPTAuOA /complete/search 13217391975440921 0 1 13201839975440921 1
1 1
13201839975440981 .google.com CGIC
lkp0ZXh0L2h0bWwsYXBwbGljYXRpb24veGh0bWwreG1sLGFWcGxpY2F0aW9uL3htbDtxPTAuOSxpb
WFNzS93ZWJwLmCovKjtxPTAuOA /search 13217391975440981 0 1 13201869034945953 1 1 1
13201839976795640 .google.com SNID APNaz9_2NvvZkMAWJXtrEX7qhv-mKNmdwph-
BF28AYFb3FLOfaefJbg_biASxOqPn103xwnO9wp53IY_tIWztg /verify 13217651176795640 1 1
13201869035140075 1 1 1
13201839976795740 .google.com NID
183=uK0YjjFpl_eZPi67hzupnvrnZ0wJrkyxx1Dawv1yZwaS-eprlW-
Nbclcls7VIHrwTj4hU_RDWlaWKssnlG24qXmkKwDVrbR-gzjGvbL9aNY6EjF3Y47sjfNcw-BOfMvR-
jCTexDmmGKLqJntK75hSwxXajJOktX48hzF-EyyMhb0 / 13217651176795740 0 1
13201869034945953 1 1 1
13201839978415926 .google.com ANID AHWqTUUnlOGzxns-
_U3iYMNPjKMFW5h24agqb3QrrINz36VxhLwqySYNVydVrR5W / 13264911978415926 0 1
13201869034945953 1 1 1
13201868915491540 www.guru99.com df5aae2adceb73c6abc67b211e30888b
6671d9ffa4f51f9571deb534a8e914ec / 0 1 1 13201868915491540 0 0 1
13201868917923272 .contextweb.com vf 1 / 13201920003923272 0 0
13201868917923272 1 1 1
13201868917923451 .contextweb.com wf 0 / 13202438403923451 0 0
13201868917923451 1 1 1
13201868917956745 .guru99.com _ga GA1.2.2018687982.1557395318 /
13264940917000000 0 0 13201868917956745 1 1 1
13201868917959035 .guru99.com _gid GA1.2.1301733801.1557395318 /
13201955317000000 0 0 13201868917959035 1 1 1
13201868917969950 .guru99.com _gat 1 / 13201868977000000 0 0 13201868917969950
1 1 1
13201868917995923 .rubiconproject.com rsid
1|ANaxY1YN4uLFRI+t3tw1PRLx9Z9aOLOagSF8XM2vaBB1+9bGLCy0A53WO+Wb26SJHKP5937GDav2
RiiMHkm5FDSv8QM61AZepS95O56KFHlmomnGE6VfPcX1S8/QNDDEXtTZwVM4d3Gv0qBIl8c3qMlu
WLikLQDOcodnpdMJvcSfibTN56B5+YWPUWU04+fAF2Zbrg== / 0 0 0 13201869078518614 0 0 1

13201868917996004 .rubiconproject.com ses15 242562^1 / 13201963202996004 0 0
13201869078518614 1 1 1
13201868917996081 .rubiconproject.com vis15 242562^1 / 13201963202996081 0 0
13201869078518614 1 1 1
13201868918012500 .adnxs.com icu
ChgltpYEAoYASABKAEw9e7P5gU4AUABSAEQ9e7P5gUYAA.. / 13209644918012500 0 1
13201869057055066 1 1 1
13201868918051844 .openx.net p_synced / 13203164918051844 0 0
13201869078510108 1 1 1
13201868918069223 www.guru99.com session_depth
www.guru99.com%3D1%7C441289839%3D1 / 13201870718000000 0 0 13201868918069223 1 1
1
13201868918215068 .advertising.com CfP 1 / 0 0 0 13201869078219874 0 0 1
13201868919616484 .guru99.com bfp_sn_rf_8b2087b102c9e3e5ffed1c1478ed8b78
https://www.google.com/ / 13569379200000000 0 0 13201868919616484 1 1 1
13201868919616578 .guru99.com bfp_sn_rt_8b2087b102c9e3e5ffed1c1478ed8b78
1557395319615 / 13569379200000000 0 0 13201868919616578 1 1 1
13201868919623052 .guru99.com bfp_sn_pl 1557395315_739302274994 /
13201870719000000 0 0 13201868919623052 1 1 1
13201868920015422 .www.guru99.com bafp 9de9c480-723f-11e9-8edc-6f5db312327e /
13569379200000000 0 0 13201868920015422 1 1 1
13201868921164457 .doubleclick.net IDE
AHWqTUmUSpmOWWBTE7zi7f4QGsGg6yr6Zah03ZBy4UPoBX7SUOj1GM9fKMBGC7t3 /
13264911883164457 0 1 13201909776070580 1 1 1
13201868921166156 .guru99.com __gads
ID=4197c8223d20a57c:T=1557395316:S=ALNI_Mb60KqQAclXOg0012RCvUEwDEoQQ /
13264940916000000 0 0 13201868921166156 1 1 1
13201868921272910 .pxlclnmdecom-a.akamaihd.net bfp_sn 1557395315_739302274994
/ 13201870719000000 0 0 13201868921272910 1 1 1
13201868921277307 .pxlclnmdecom-a.akamaihd.net
bfp_sn_t_8b2087b102c9e3e5ffed1c1478ed8b78
1557395315_739302274994_8b2087b102c9e3e5ffed1c1478ed8b78 / 13201870719000000 0 0
13201868921277307 1 1 1
13201868921282655 .pxlclnmdecom-a.akamaihd.net
bfp_sn_td_a7ccc199e29741c0141fa6e8fe061a9d
1557395315_739302274994_a7ccc199e29741c0141fa6e8fe061a9d / 13201870719000000 0 0
13201868921282655 1 1 1
13201868921743137 .pxlclnmdecom-a.akamaihd.net bafp_t 9ed276d0-723f-11e9-b453-
b767521ec807 / 13569379200000000 0 0 13201868921743137 1 1 1
13201868922556417 .smartadserver.com pid 547233617597203728 /
13236169722556417 0 0 13201868922556417 1 1 1
13201868922556527 .smartadserver.com TestIfCookieP ok / 13236169722556527 0 0
13201868922556527 1 1 1
13201868922945214 .simpli.fi uid qT1n8VzT93iWLyCjbm/8Ag== / 13233491322945214 0 0
13201868922945214 1 1 1
13201868922984781 .mathtag.com mt_mop 4:1557395320 / 13204460922984781 0 0
13201869057569150 1 1 1

13201868923048458 .adhigh.net gi_u 5BLOi0VJNB / 13233404923048458 0 0
13201868923048458 1 1 1
13201868923219456 .pubmatic.com KADUSERCOOKIE 68C49BCB-FB7D-4142-AE4A-
32D28E2B7C0C / 13209644923219456 0 0 13201869078516357 1 1 1
13201868923219727 image6.pubmatic.com f5_cspm 1234 /AdServer 0 0 0
13201869078516357 0 0 1
13201868923486715 .netmng.com dsp_id ngnjowuymwvhm / 13217680123486715 0 0
13201868923486715 1 1 1
13201868923691539 .pubmatic.com KRTBCOOKIE_80 16514-CAESEH3DBqteW6LenAsZjh-
G2_c&KRTB&22987-CAESEH3DBqteW6LenAsZjh-G2_c&KRTB&22995-CAESEH3DBqteW6LenAsZjh-
G2_c / 13209644923691539 0 0 13201869078516357 1 1 1
13201868923935051 .pubmatic.com KRTBCOOKIE_27 16735-uid:c2a05cd3-7de7-4e00-
86bd-d44dd1db56bd&KRTB&16736-uid:c2a05cd3-7de7-4e00-86bd-d44dd1db56bd /
13204460923935051 0 0 13201869078516357 1 1 1
13201868923936827 .pubmatic.com KRTBCOOKIE_377 6810-34d16a20-60b6-4f2f-8a2b-
0b034462daa7&KRTB&22918-34d16a20-60b6-4f2f-8a2b-0b034462daa7&KRTB&23031-34d16a20-
60b6-4f2f-8a2b-0b034462daa7 / 13209644923936827 0 0 13201869078516357 1 1 1
13201868923938757 .pubmatic.com KRTBCOOKIE_22 14911-
4132403619155936041&KRTB&16087-4132403619155936041&KRTB&23049-
4132403619155936041 / 13204460923938757 0 0 13201869078516357 1 1 1
13201868923972345 .pubmatic.com KRTBCOOKIE_218 4056-
XNP3eAAAAKEkHjve&KRTB&22922-XNP3eAAAAKEkHjve&KRTB&22978-XNP3eAAAAKEkHjve /
13209644923972345 0 0 13201869078516357 1 1 1
13201868924077477 .pubmatic.com KRTBCOOKIE_330 22938-
220290e6adea1f392c8e6cc18707a2f4&KRTB&22939-220290e6adea1f392c8e6cc18707a2f4 /
13204460924077477 0 0 13201869078516357 1 1 1
13201868924225031 bh.contextweb.com _dbefe http://10.204.71.19:8080 / 0 0 0
13201868924225031 0 0 1
13201868924227316 .pubmatic.com KTPCACOOKIE YES / 13209644924000000 0 0
13201869078516357 1 1 1
13201868924262370 .pubmatic.com DPSync2
1557964800%3A164%7C1557446400%3A174%7C1558569600%3A197_201_200 /
13209644924262370 0 0 13201869078516357 1 1 1
13201868924262445 .pubmatic.com SyncRTB2
1558569600%3A3_55_104_8_54_64_71_166_7_189_22_13_21%7C1558656000%3A35%7C15576
19200%3A160%7C1557964800%3A2 / 13209644924262445 0 0 13201869078516357 1 1 1
13201868924496367 .adform.net uid 5050868504865421025 / 13207052924496367 0 0
13201868924496367 1 1 1
13201868924527323 .ipredictive.com cu a0ba4a5e-723f-11e9-95fb-
4f79de10005f|1557395321658 / 13233404925527323 0 0 13201868924527323 1 1 1
13201868924563535 .turn.com uid 4132403619155936041 / 13217420924563535 0 0
13201868924563535 1 1 1
13201868924610161 .gumgum.com vst u_aa4d1938-773c-4225-9964-b1fc9296aff6 /
13233404924610161 0 0 13201868924610161 1 1 1
13201868924614302 .pubmatic.com KRTBCOOKIE_57 22767-
311972100389478579&KRTB&22776-311972100389478579 / 13209644924614302 0 0
13201869078516357 1 1 1

13201868924641695 .pubmatic.com KRTBCOOKIE_148 19421-
uid:F1673DA978F7D35CA3202F9602FC6F6E / 13204460924641695 0 0 13201869078516357 1 1 1
13201868924804438 .pubmatic.com KRTBCOOKIE_153 19420-
Yl1XuW3YAut43QDobdYeuTfZUbp41gG4Y9wEk7ct&KRTB&22979-
Yl1XuW3YAut43QDobdYeuTfZUbp41gG4Y9wEk7ct / 13209644924804438 0 0 13201869078516357
1 1 1
13201868924849978 .pubmatic.com KRTBCOOKIE_279 22890-a0ba4a5e-723f-11e9-95fb-
4f79de10005f / 13204460924849978 0 0 13201869078516357 1 1 1
13201868924852764 .pubmatic.com KRTBCOOKIE_1074 22956-u_aa4d1938-773c-4225-
9964-b1fc9296aff6 / 13204460924852764 0 0 13201869078516357 1 1 1
13201868924872140 .bidr.io bito AASPtK65p-8AABe2JAK-Uw / 13264926524872140 0 0
13201868924872140 1 1 1
13201868924877729 .openx.net univ_id 537072971|34d16a20-60b6-4f2f-8a2b-
0b034462daa7|1557395322021406 / 13203164924877729 0 0 13201869078510108 1 1 1
13201868924916284 .pubmatic.com KRTBCOOKIE_188 3189-05a43920-9642-4696-89c9-
002b70371119&KRTB&22716-05a43920-9642-4696-89c9-002b70371119 / 13217420924916284 0
0 13201869078516357 1 1 1
13201868924999760 .owneriq.net si Q6106817222026235973 / 13359548924999760 0 0
13201868924999760 1 1 1
13201868924999863 .owneriq.net p2 cwc / 13202732924999863 0 0 13201868924999863
1 1 1
13201868925028963 .pubmatic.com KRTBCOOKIE_1030 22848-k55Pa5oXtm4J /
13204460925028963 0 0 13201869078516357 1 1 1
13201868925059184 .advertising.com IDSYNC "18bj~1khl:17kh~1khl:176s~1khl" /
13233491325059184 0 0 13201869078219874 1 1 1
13201868925072175 .taboola.com t_gid 1c23606c-4e37-41e1-8011-5365947b14a0-
tuct3cd7cfa / 13233404925072175 0 0 13201868925072175 1 1 1
13201868925107386 eus.rubiconproject.com pux
1512%3D81964%262238%3D81964%262249%3D81964%262307%3D81964%262974%3D81964%2
63778%3D81964%26goog%3D81964%26brx%3D81964%26 / 13209644925000000 0 0
13201868925107386 1 1 1
13201868925148380 .bidswitch.net c 1557395322 / 13233404925148380 0 0
13201868925148380 1 1 1
13201868925197746 .c.bing.com ANONCHK 1 / 13201869526197746 0 0
13201868925197746 1 1 1
13201868925197822 .bing.com MUID 1C8E4FBBC90B68010DE742ECCD0B6BD7 /
13235564926197822 0 0 13201868925197822 1 1 1
13201868925197883 .c.bing.com MR 0 / 13217420926197883 0 0 13201868925197883 1
1 1
13201868925197945 c.bing.com MUIDB 2090BA11A94762E30F7CB746A8C56350 /
13235564926197945 0 1 13201868925197945 1 1 1
13201868925239948 .sharethrough.com stx_user_id a19cffe8-d5a9-48c7-b428-
820a224bbec4 / 13233404922000000 0 0 13201868925239948 1 1 1
13201868925244756 .bidswitch.net tuuid 54fb1e26-7eeb-4b31-9891-391e3929fb7e /
13233404925244756 0 0 13201868925244756 1 1 1
13201868925244856 .bidswitch.net tuuid_lu 1557395322 / 13233404925244856 0 0
13201868925244856 1 1 1

13201868925292658 .3lift.com tluid 12025328567121464445 / 13209644925292658 0 0
13201868925292658 1 1 1
13201868925325334 cks.mynativeplatform.com JSESSIONID
EACFD5C99E1B69014A35C2AC7E91027F.nodePub20 / 0 0 0 13201868925325334 0 0 1
13201868925325394 .mynativeplatform.com glck_pulsepoint_ck k55Pa5oXtm4J#D /
13359548925325394 0 0 13201868925325394 1 1 1
13201868925325455 .mynativeplatform.com glck 5cd3f77ae4b010cf3aca091a#D /
13359548925325455 0 0 13201868925325455 1 1 1
13201868925393544 .s3xified.com admRtbUidCkey34334Ssp245
62658c391f5543b55c6bd33d3bc29707 / 13517228925393544 0 0 13201868925393544 1 1 1
13201868925408017 .zorosrv.com cicouid CM_1c23606c-4e37-41e1-8011-5365947b14a0-
tuct3cd7cfa / 13233404925408017 0 0 13201868925408017 1 1 1
13201868925439098 .ads.deliverimp.com buid_r_ppnt k55Pa5oXtm4J /
13209644925439098 0 1 13201868925439098 1 1 1
13201868925439254 .ads.deliverimp.com cuid 11964924011557395322 /
13209644925439254 0 1 13201868925439254 1 1 1
13201868925460319 .smartadserver.com csync
76:CAESEGBYvie3vSxMBAUyfGj8GEM|127:AASptk65p-8AABe2JAK-Uw / 13236169725460319 0 0
13201868925460319 1 1 1
13201868925462304 .254a.com tuuid 1de25d76-f715-4d40-93af-27ec878ea77b /
13209644925462304 0 0 13201868925462304 1 1 1
13201868925462379 .254a.com tuuid_lu 1557395322 / 13209644925462379 0 0
13201868925462379 1 1 1
13201868925473264 pool.admedo.com tuuid ce5c2d73-b661-4aa6-afa6-63ede5c38851 /
13233404925473264 0 0 13201868925473264 1 1 1
13201868925473333 pool.admedo.com tuuid_lu 1557395322 / 13233404925473333 0 0
13201868925473333 1 1 1
13201868925535084 .mobileadtrading.com SOMOID
602a38e81b404ff0aa38e81b406ff048 / 13203164925535084 0 0 13201868925535084 1 1 1
13201868925540070 .altitude-arena.com um
"!8mk6u4tbg157pa64cvsm12pjng,k55Pa5oXtm4J" / 13204460925540070 0 0 13201868925540070
1 1 1
13201868925650141 .1rx.io _rxuuid %7B%22rx_uuid%22%3A%22RX-c2ea4463-b99e-
4652-9c04-8aa4cae6623d%22%2C%22nxtrdr%22%3Afalse%7D / 13233404925650141 0 1
13201868925650141 1 1 1
13201868925705139 .media.net visitor-id 2003969229148392000V10 /
13233404925705139 0 0 13201868925705139 1 1 1
13201868925705227 .media.net data-p k55Pa5oXtm4J~~3 / 13232108925705227 0 0
13201868925705227 1 1 1
13201868925765745 .vertamedia.com vmuid 4c51023954c9abee / 13207225726765745 0
0 13201868925765745 1 1 1
13201868925765819 .vertamedia.com e0 k55Pa5oXtm4J / 13207225726765819 0 0
13201868925765819 1 1 1
13201868925775259 partners.tremorhub.com AWSELB
BD5F01E3168F81D64F20FC737D53DAE6B1E3FB62EC0F3A07B585EC484F889D36349B0798DEC876
152D2CA7057D9F344D02E05829D45BA83F3F67CA710762A6387D2FCD9A5C /
13201868945775259 0 0 13201868925775259 1 1 1

13201868925783357 .smrtb.com __cfduid
d525c3206b696f27b053b8f28a720c4881557395322 / 13233404925783357 0 1
13201868925783357 1 1 1
13201868925813127 .rubiconproject.com put_5412 k55Pa5oXtm4J / 13204288125813127
0 0 13201869078518614 1 1 1
13201868925822928 .pubmatic.com KRTBCOOKIE_699 22727-AASPtK65p-8AABe2JAK-
Uw&KRTB&22744-AASPtK65p-8AABe2JAK-Uw&KRTB&22745-AASPtK65p-8AABe2JAK-Uw /
13204460925822928 0 0 13201869078516357 1 1 1
13201868925863132 .teads.tv tt_viewer a6c93d63-22a3-4948-bbaa-ee5d4089048a /
13233318525863132 0 0 13201868925863132 1 1 1
13201868925875310 .videostat.com uid 570b4c86be36c7f539039dd435090625 /
13204460925875310 0 0 13201868925875310 1 1 1
13201868925875384 .videostat.com id 570b4c86be36c7f539039dd435090625 /
13204460925875384 0 0 13201868925875384 1 1 1
13201868925896514 .media.net mnetCppt k55Pa5oXtm4J*350 / 0 0 0
13201868925896514 0 0 1
13201868925953633 .yieldmo.com yieldmo_id
gf98095f02f96e0942ac%7C1557395323091%7C0%7C / 13233404925953633 0 0
13201868925953633 1 1 1
13201868925953832 .ads.yieldmo.com ptrpp k55Pa5oXtm4J / 13233404925953832 0 0
13201868925953832 1 1 1
13201868926025101 .targeting.unrulymedia.com unruly_m11
NHAObvOz/cCzDmkYTbs41A== / 13202473726025101 0 0 13201868926025101 1 1 1
13201868926164810 .rubiconproject.com put_5120 k55Pa5oXtm4J / 13204374526164810
0 0 13201869078518614 1 1 1
13201868926381376 .lfstmedia.com adm_t78Q8VC3dzbmt-t0SgOakg
P3v6prx1Z5iCFJL9CEGGZw0lyQTYzODX282LcOdqW2k3aDGWEjuhlqDRy01NOQdTAM1okO+jgT+zX8
M_4akaloOwplBCGjVNrJDYRddplw4O2Y9DgXWemFRATJrNp8WB4+IRN+nQaPo- /
13264940926381376 0 0 13201868926381376 1 1 1
13201868926384401 .lfstmedia.com adm_t78Q8VC3dzazWzcFEarT8OPiETfp0Gj6
P3v6prx1Z5iCFJL9CEGGZw0lyQTYzODX282LcOdqW2n4tvZKRQBe0BsnzCFuAaNxIWmiyEs9SYj4AothZ
sgl6_U+OGHJKc4_dn8Nmjr7sncjeMG4omjtpuXrVPq+GqMEBP93EU4mA7pbaow9mCGlp+2eJP6JNbr
aCowAAuuY7bMyBZcar4hl5A-- / 13264940926384401 0 0 13201868926384401 1 1 1
13201868926482731 .erne.co u LeyFvhIDEWfONtvuErPVSwus / 13264940926482731 0 0
13201868926482731 1 1 1
13201868926613515 .videmob.com vm_usp1037
d9KTpTwBwtwSHFHzUWCNhMRH8S%2BrpK23y7g2YG%2BzxGs / 13233404926613515 0 0
13201868926613515 1 1 1
13201868926613735 .videmob.com vm_usv
9qLwNEJkEuz2wCLDQgEdJh33mDYMT7vyzKZ9ch%2B%2F0q4%2FkmQLHcmHdZvM4hgof5n6 /
13233404926613735 0 0 13201868926613735 1 1 1
13201868926664642 .mediabong.net _plsp k55Pa5oXtm4J / 13201955326664642 0 0
13201868926664642 1 1 1
13201868926664843 .mediabong.net _mb 1218cc4a825608a8 / 0 0 0
13201868926664843 0 0 1
13201868926972462 .casalemedia.com CMRUM3 bd5cd3f77c2760k55Pa5oXtm4J /
13233404926972462 0 0 13201869057583269 1 1 1

13201868926979706 .pubmatic.com KRTBCOOKIE_466 16530-54fb1e26-7eeb-4b31-9891-391e3929fb7e&KRTB&16532-54fb1e26-7eeb-4b31-9891-391e3929fb7e / 13204460926979706 0 0
13201869078516357 1 1 1
13201868926981384 .pubmatic.com PugT 1557395324 / 13204460926981384 0 0
13201869078516357 1 1 1
13201868926982030 .pubmatic.com PUBMDCID 1 / 13209644926982030 0 0
13201869078516357 1 1 1
13201868926982313 simage2.pubmatic.com f5_cspm 1234 /AdServer 0 0 0
13201868926982313 0 0 1
13201868926984441 .adsnative.com __cfduid
d1b09a449e49fec12b916c421838604ff1557395324 / 13233404926984441 0 1
13201868926984441 1 1 1
13201868927153228 .pubmatic.com SPugT 1557395324 / 13204460927153228 0 0
13201869078516357 1 1 1
13201868927431301 .quantserve.com d EAgBFwHEHYEADfkWz53BAA /
13209644927431301 0 0 13201869076617658 1 1 1
13201868927440301 .dotomi.com DotomiUser 716504932211662772\$3\$1633313514\$\$1
/ 13235824127440301 0 0 13201868927440301 1 1 1
13201868927479910 .kargo.com ktcid aece4c97-fdd7-46b2-ba97-a58d94b2212b /
13517228927479910 0 0 13201868927479910 1 1 1
13201868927488605 .spotxchange.com audience 9f797a80-723f-11e9-8295-
1b8927d51103 / 13204460927488605 0 0 13201868927488605 1 1 1
13201868927496414 .mookie1.com syncdata_AN 1 / 13202732927496414 0 0
13201869083561900 1 1 1
13201868927613249 .adnxs.com anj
dTM7k!M40uEs8>[F']wlg2llheloFo!j6N5e4S`8h_6lpIDHj:1wfT@!xxjyF0)_^sX6OWJy2P3bYciSQMZtp
lvsHBNQe9>\$6ILYBoE'j-MBX@bmCB?F/eL)\$6AuN(_9#f+Uz9<x?u'!Qa3jOq`nlgKT^/j6N/h-
.7G4B)Q#jd@PQ.'Va[7^Sml:S:E'-
#h*aBX1Nv:^\./KOtr+s#u)#pfm%rH<Tw'eh?CY7oX1Fa?8N2>okaWS15fS)sWpIP=JB3eCnY3Z[.X-4 /
13209644927613249 0 1 13201869057055066 1 1 1
13201868927786098 .onaudience.com cookie 27f6cb4a106e8b92 / 13233404927786098
0 0 13201868927786098 1 1 1
13201868927786233 .onaudience.com done_redirects104 1 / 13201955327786233 0 0
13201868927786233 1 1 1
13201868927827042 .adsrvr.org TDID 34d16a20-60b6-4f2f-8a2b-0b034462daa7 /
13233491327827042 0 0 13201868927827042 1 1 1
13201868927827236 .adsrvr.org TDCPM
CAESFwoIcHVibWF0aWMSCwje9ublsZuqNxAFEhKkCmRyYXdicmlkZ2USCwiMwd_LsZuqNxAFEhQKB
W9wZW54EgslpvDp1LgbqjcQBRIXCghhcHBuZXh1cxILCLCpk--
xm6o3EAUSFgoHcnViaWNvbhlLCIDzKfCxm6o3EAUSGAoJbW9va2llXBzEgslzNbp8rGbjcQBRgBIAEo
AjlLCmzO7J_lm6o3EAU4AVoJbW9va2llXBzYAI. / 13233491327827236 0 0 13201868927827236 1
1 1
13201868927834145 .rubiconproject.com put_2307 34d16a20-60b6-4f2f-8a2b-
0b034462daa7 / 13204288127834145 0 0 13201869078518614 1 1 1
13201868927939911 .mookie1.com syncdata_TTD 1 / 13202732927939911 0 0
13201869083561900 1 1 1
13201868927963691 .rubiconproject.com put_1512 c2a05cd3-7de7-4e00-86bd-
d44dd1db56bd / 13204374528963691 0 0 13201869078518614 1 1 1

13201868927972097 .rubiconproject.com put_3778 XNP3eAAAAKEkHjve /
13204374528972097 0 0 13201869078518614 1 1 1
13201868928175779 .yahoo.com B 09d3l9ped7trp&b=3&s=1m / 13233404928175779 0 0
13201868928175779 1 1 1
13201868928302126 .sitescout.com ssi 05a43920-9642-4696-89c9-002b70371119 /
13233404928302126 0 0 13201868928302126 1 1 1
13201868928302258 .sitescout.com _ssum
eyl1ljoxNTU3Mzk1MzlyMDMwLCI3ljoxNTU3Mzk1MzlyMDMwfQ / 13204460928302258 0 0
13201868928302258 1 1 1
13201868928304851 .mookie1.com syncdata_DBC 1 / 13202732928304851 0 0
13201869083561900 1 1 1
13201868928314218 .rubiconproject.com put_2974 6636651496518050852 /
13204374529314218 0 0 13201869078518614 1 1 1
13201868928342227 pixel-us-east.rubiconproject.com audit
"exG/kKnanCGx5Sp9+I9NVXHBuWaPvA5ZNJhyv00WO+CZUdazYKDv6GL7uyUxe5hWjl/9KaCmwO/R
Zgr6h/0AJDqT71/0NjTAiw970A6WYyafdH/ssR4wGA==" /exchange 13233404927342227 0 0
13201868928342227 1 1 1
13201868928406990 .rubiconproject.com put_2238 05a43920-9642-4696-89c9-
002b70371119 / 13204288129406990 0 0 13201869078518614 1 1 1
13201868928414311 .tapad.com TapAd_TS 1557395322501 / 13207052928414311 0 0
13201868928414311 1 1 1
13201868928414501 .tapad.com TapAd_DID a13aeb51-723f-11e9-826e-3e5450dcf4d4 /
13207052928414501 0 0 13201868928414501 1 1 1
13201868928417701 .crwdcntrl.net _cc_dc 0 / 13225196928417701 0 0
13201868928417701 1 1 1
13201868928417824 .crwdcntrl.net _cc_id 94f1357715aa57c489c5666eca5991e8 /
13225196928417824 0 0 13201868928417824 1 1 1
13201868928417921 .crwdcntrl.net _cc_cc
"ACZ4nGNQsDRJMzQ2NTc3NE1MNDVPNrGwTDY1MzNLTU40tbQ0TLVgAIKYy99rGRAAAE1BCXI%3D
" / 13225196928417921 0 0 13201868928417921 1 1 1
13201868928418026 .crwdcntrl.net _cc_aud "ABR4nGNgYGClufy9lgEOACDEAqQ%3D" /
13225196928418026 0 0 13201868928418026 1 1 1
13201868928485909 .mookie1.com syncdata_TAP 1 / 13202732928485909 0 0
13201869083561900 1 1 1
13201868928671172 .mookie1.com syncdata_ADF 1 / 13202732928671172 0 0
13201869083561900 1 1 1
13201868928867440 .w55c.net matchgroupm 5 / 13204460929867440 0 0
13201869057573159 1 1 1
13201868928913940 .mookie1.com syncdata_DAT 1 / 13202732928913940 0 0
13201869083561900 1 1 1
13201868929107328 .contextweb.com V k55Pa5oXtm4J / 13232972929107328 0 0
13201868929107328 1 1 1
13201868929107498 .contextweb.com pb_rtb_ev 3-
tfg|7E9.0|7Ot.0.x/BHnKRUIqte/BFBER5f3DCkz|7C6.0.570b4c86be36c7f539039dd435090625|7fp
.0|7Eb.0|7YQ.0.22e532aa-f177-44c4-c49f-
f2bd9f2b1fd0|79f.0.EHbmcB0jsyllJrEhHS2vcEci4HMLbBxEyeFFnZv|7hx.0|7jM.0|Vs.0.34d16a20-
60b6-4f2f-8a2b-
0b034462daa7|77s.0|7hN.0|7fK.0|7Cs.0|7br.0|7bs.0|7WX.0|87i.0|7Xh.0|83u.0|-

5.0|7i3.0|7N2.0|87G.0|6T6.0|7As.0|7KO.0.4ff21de5-23cb-4318-b06a-
92cd3b857607|77B.0|7dN.0.AASPTk65p-8AABe2JAK-
Uw|7hV.0.62658c391f5543b55c6bd33d3bc29707|85M.0|4is.0.CAESEB1DHuGu7fMa8GzZhUrOgdg
|7Rn.0.LeyFvhIDEWfONTvuErPVSwus|3oy.0.05a43920-9642-4696-89c9-
002b70371119|3qC.0|0.0|81B.0|88b.0|6XH.0|7Tw.0|7ef.0|7Ty.0|2JB.0|aE.0|7Nq.0|7Bj.0.CAESE
APipirG46ytp-
FyC5LH1_s|86h.0.959900041323373705|7VZ.0|7aw.0|7TY.0|7TZ.0|88e.0|7FI.0|7NB.0|824.0|7Fn
.0|7Yi.0.438d44681ed0ba85e0e7ad5e57830222|14X.0|6zB.0.54fb1e26-7eeb-4b31-9891-
391e3929fb7e|78K.0.RX-c2ea4463-b99e-4652-9c04-
8aa4cae6623d|7Wk.0|2N.0.AQEI8lhXjUuetQJgW2PrAQEBAQE|7Dw.0|7RY.0|1Em.0.F1673DA978F
7D35CA3202F9602FC6F6E|17m.0.HjuxKlk51HoFFo5|4Ec.0|76Y.0|86H.0|5Ql.0.1c23606c-4e37-
41e1-8011-5365947b14a0-tuct3cd7cfa|86L.0|7DS.0 / 13233404929107498 0 0
13201868929107498 1 1 1
13201868931591889 www.guru99.com _omappvp
KmNu9wixlPbD9o8dj953rUt1TaYb1YYCrrZOSChadFvcxeSuq8dnVzGUWcDURMRLb3IK90x7keFQK8hl
sPy6vVtwTSyD23gw / 13547382531000000 0 0 13201868931591889 1 1 1
13201868931593217 www.guru99.com _omappvs 1557395331588 / 13201869531000000
0 0 13201868931593217 1 1 1
13201868954461496 resources.infosecinstitute.com infosec_post_order
ORDER_DATE_DESC /10-popular-password-cracking-tools 0 0 0 13201869015919676 0 0 1
13201868955493266 .onesignal.com __cfduid
db0cb30c4f064ae064ea9466f2a4504921557395352 / 13233404955493266 0 1
13201868955493266 1 1 1
13201868956053111 go.pardot.com pardot ma2up5gjfrplrfdmqhvc8n85f2 / 0 0 0
13201868956053111 0 0 1
13201868956385875 resources.infosecinstitute.com _omappvp
SgLRw8Slvc28okV0C3Q91BYlZNS5AUX4FnTWzy523cUNIZ1Af6QGTKikOBHxhDJgrkT2MjyDXd2Eo9v7
pekeJS5kgD51coMB / 13547382556000000 0 0 13201869017994165 1 1 1
13201868956386881 resources.infosecinstitute.com _omappvs 1557395356379 /
13201869556000000 0 0 13201869017994165 1 1 1
13201868964386997 .twitter.com tfw_exp 0 / 13203078564386997 0 0
13201868964386997 1 1 1
13201868965707585 pi.pardot.com pardot 7om3dig6sk8fp0tg7trsh4o2a0 / 0 0 0
13201868965707585 0 0 1
13201868966231258 go.pardot.com visitor_id12882 512689884 / 13517228966000000 0
0 13201868966231258 1 1 1
13201868966242788 go.pardot.com visitor_id12882-hash
eb516048e2ae9bc583fec3709ced06da6791f5fcc791a2545f8fb47a799ccf53f046f452aae7302feb7a
99f885842b8848e8af0e / 13517228966000000 0 0 13201868966242788 1 1 1
13201868966419196 www2.infosecinstitute.com pardot vmhn8b44kp8ai3uijobom4nd62 /
0 0 0 13201868966419196 0 0 1
13201868967300032 .ads.linkedin.com BizolD 802f26ef-0a05-46a9-a973-a8bc883fd02d /
13204460967300032 1 0 13201868967300032 1 1 1
13201868967300121 .ads.linkedin.com lang v=2&lang=en-us / 0 0 0 13201868967300121
0 0 1
13201868967300181 .linkedin.com lidc
"b=TGST00:g=1588:u=1:i=1557395364:t=1557481764:s=AQEnPuG3veZe9eMfJHrQYHfTjyQYIXh6" /
13201955367300181 0 0 13201868967300181 1 1 1

13201868967372548 .linkedin.com UserMatchHistory
AQJwFRWPXkjlUwAAAWqb_1qU7H55W3S6O0rmNyFR2SckbldYdBCCJdfhPyBbRa73m9x5s8oAi8 /
13204460967372548 1 0 13201868967372548 1 1 1
13201868967408244 .infosecinstitute.com _ga GA1.2.1309105245.1557395365 /
13264940967000000 0 0 13201869032671845 1 1 1
13201868967410272 .infosecinstitute.com _gid GA1.2.75243750.1557395365 /
13201955367000000 0 0 13201869032671845 1 1 1
13201868967505005 .pardot.com visitor_id12882 512689884 / 13517228967505005 0 0
13201868967505005 1 1 1
13201868967505078 .pardot.com visitor_id12882-hash
eb516048e2ae9bc583fec3709ced06da6791f5fcc791a2545f8fb47a799ccf53f046f452aae7302feb7a
99f885842b8848e8af0e / 13517228967505078 0 0 13201868967505078 1 1 1
13201868967505138 pi.pardot.com lpv12882
aHR0cHM6Ly9yZXNvdXJjZXMuW5mb3NiY2luc3RpdHV0ZS5jb20vMTAtcG9wdWxhci1wYXNzd29yZ
C1jcmFja2luZy10b29scy8jZjZg%3D%3D / 13201870767505138 0 0 13201868967505138 1 1 1
13201868967697707 .linkedin.com lang v=2&lang=en-us / 0 0 0 13201868967697707 0 0 1
13201868967697793 .linkedin.com bcookie "v=2&7e402919-a1de-43ac-8935-
58c99513602a" / 13264982819697793 0 0 13201868967697793 1 1 1
13201868967697876 .www.linkedin.com bscookie "v=1&20190509094924e564380d-3ed4-
4ec1-8722-02595afa4802AQGyoQUV6XwpG-k3xYAtg2b2Y3TTWGJf" / 13264982819697876 1 1
13201868967697876 1 1 1
13201868967709394 resources.infosecinstitute.com visitor_id12882 512689884 /
13517228967000000 0 0 13201869032671845 1 1 1
13201868967709910 resources.infosecinstitute.com visitor_id12882-hash
eb516048e2ae9bc583fec3709ced06da6791f5fcc791a2545f8fb47a799ccf53f046f452aae7302feb7a
99f885842b8848e8af0e / 13517228967000000 0 0 13201869032671845 1 1 1
13201868967772586 www2.infosecinstitute.com visitor_id12882 512689884 /
13517228967772586 0 0 13201868967772586 1 1 1
13201868967772676 www2.infosecinstitute.com visitor_id12882-hash
bc3dcf717168500e4599952ad93122c70b15cc73938dd474d91510cfc37e59ff97b7c1d3c9dcc5ef7b
89570fc45fa416a2bc55bf / 13517228967772676 0 0 13201868967772676 1 1 1
13201868983020728 .infosecinstitute.com _fbp fb.1.1557395366302.356415384 /
13209644983000000 0 0 13201868983020728 1 1 1
13201869037500498 www.google.com DV 48aBDJ_ueCAi0PXn5VxrPeJFK1CkqZa-
nAXwuGDLXAEAAAA / 13201869637000000 0 0 13201869037500498 1 1 1
13201869044159981 .google.com 1P_JAR 2019-05-09-09 / 13204461044159981 0 0
13201869044159981 1 1 1
13201869045995843 .hackaday.com _gat_HD467 1 / 13201869105000000 0 0
13201869045995843 1 1 1
13201869046023283 .hackaday.com _gat_HD466 1 / 13201869106000000 0 0
13201869046023283 1 1 1
13201869046052280 .hackaday.com _gat_HD468 1 / 13201869106000000 0 0
13201869046052280 1 1 1
13201869046091888 .hackaday.com _gat_HD465 1 / 13201869106000000 0 0
13201869046091888 1 1 1
13201869046308567 .hackaday.com _ga GA1.2.1901285592.1557366330 /
13264941046000000 0 0 13201869046308567 1 1 1

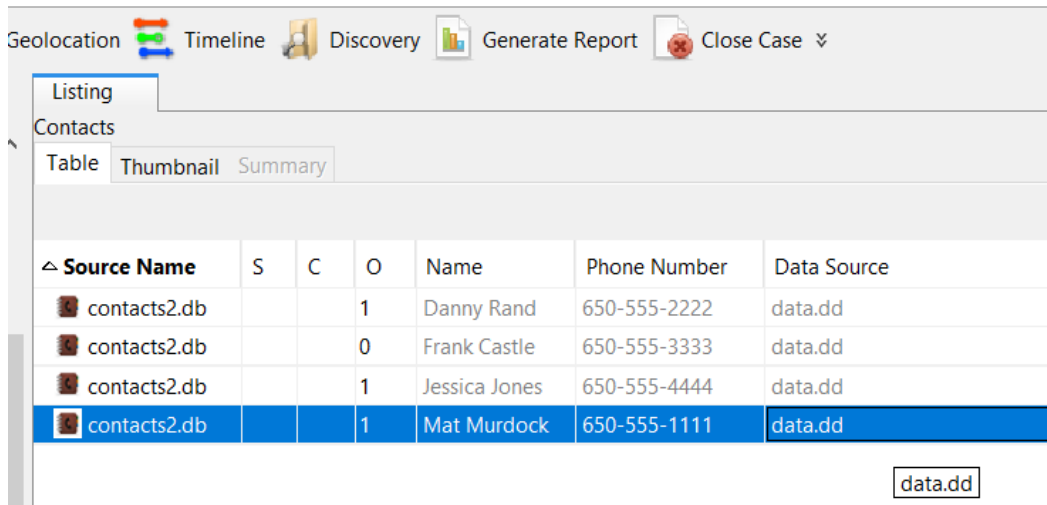
[illegible]

- **La lista de contactos**

Según la lista del dispositivo utilizando Autopsy adjunto lista:

- 1- Danny Rand 650-555-2222
- 2- Frank Castle 650-555-3333
- 3- Jessica Jones 650-555-4444
- 4- Mat Murdock 650-555-1111

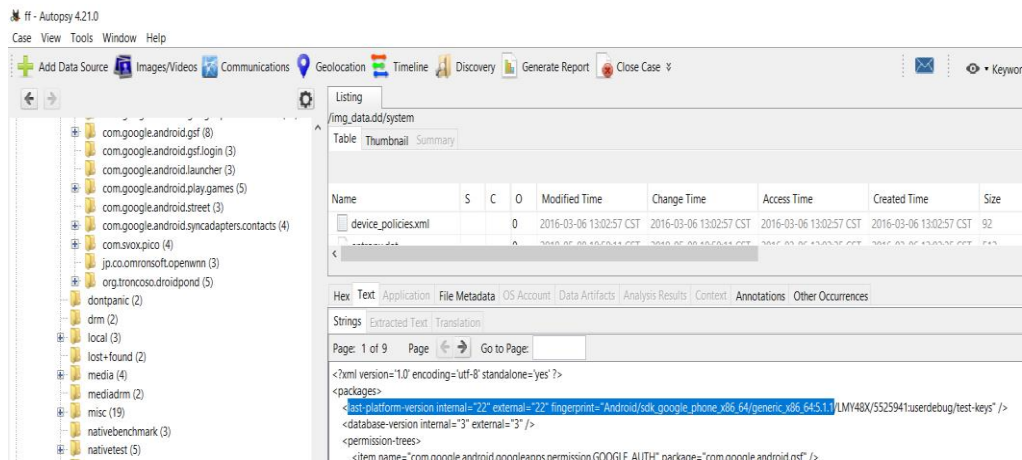
Imagen de los resultados.



Source Name	S	C	O	Name	Phone Number	Data Source
contacts2.db			1	Danny Rand	650-555-2222	data.dd
contacts2.db			0	Frank Castle	650-555-3333	data.dd
contacts2.db			1	Jessica Jones	650-555-4444	data.dd
contacts2.db			1	Mat Murdock	650-555-1111	data.dd

- **Versión del sistema operativo del celular**

Android Lollipop según lo encontrado en la carpeta System utilizando el programa Autopsy.



ff - Autopsy 4.21.0
Case View Tools Window Help

Listing
/img_data.dd/system

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
device_policies.xml			0	2016-03-06 13:02:57 CST	2016-03-06 13:02:57 CST	2016-03-06 13:02:57 CST	2016-03-06 13:02:57 CST	92
system_data			0	2016-03-06 13:02:57 CST	2016-03-06 13:02:57 CST	2016-03-06 13:02:57 CST	2016-03-06 13:02:57 CST	143

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings
Page: 1 of 9
Go to Page:

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<packages>
  <platform-version internal="22" external="22" fingerprint="Android/sdk_google_phone_x86_64/generic_x86_64/5.1.1/LM148X/5525941/userdebug/test-keys" />
  <database-version internal="3" external="3" />
  <permission-trees>
    <item name="com.google.android.googleapps.permission.GOOGLE_AUTH" package="com.google.android.gsf" />
  </permission-trees>
</packages>
```


Y buscando en la web para identificar la versión del OS.

Todo	Videos	Noticias	Shopping	Imágenes	⋮ Más	Herramientas
<hr/>						
Android Lollipop						
<hr/>						
Última versión estable		5.1.1 (LMY49M) (info) (5 de julio de 2016 (7 años, 10 meses y 20 días))				
<hr/>						
Serie Android						
<hr/>						
Android 4.4 "KitKat"		Android Lollipop		Android 6.0 "Marshmallow"		
<hr/>						
Asistencia técnica						

- **Aplicaciones instaladas**

Me dirijo en en el sistema Autopsy y encuentro la carpeta con el nombre APP.

Adjunto lista de algunas aplicaciones instaladas:

ApiDemos.apk

CubeLiveWallpapers.apk

GestureBuilder.apk

Name	Size	Flags(Dir)	Flags(Meta)
[parent folder]			
ApiDemos	4096	Allocated	Allocated
CubeLiveWallpapers	4096	Allocated	Allocated
GestureBuilder	4096	Allocated	Allocated
org.troncoso.droidpond-1	4096	Allocated	Allocated
org.troncoso.droidpond-1	4096	Unallocated	Allocated
SmokeTest	4096	Allocated	Allocated
SmokeTestApp	4096	Allocated	Allocated
SoftKeyboard	4096	Allocated	Allocated
vmdt211569852.tmp	4096	Unallocated	Allocated
WidgetPreview	4096	Allocated	Allocated
org.troncoso.droidpond-2	60	Unallocated	Allocated
org.troncoso.smart-2	0	Unallocated	Allocated

- Cuentas registradas

Encuentro solamente una cuenta registrada:

ceupe.forensics@gmail.com

ff - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

/img_data.dd/system/users/0

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
------	---	---	---	---------------	-------------	-------------	--------------

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

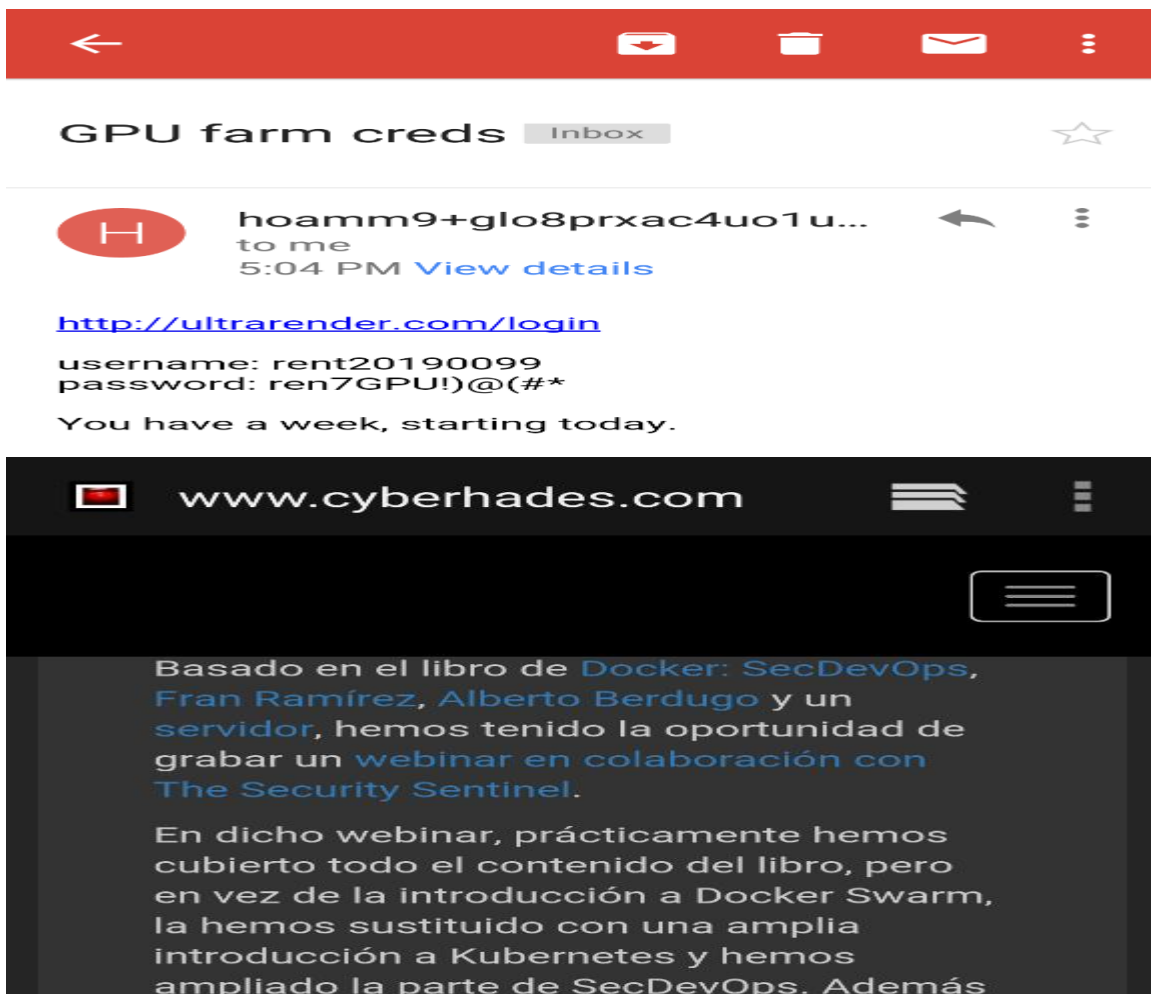
Table accounts 1 entries Page 1 of 1 Export to CSV

_id	name	type	password	pr
1	ceupe.forensics@gmail.com	com.google	aas_et/AKpplNbwNIRHosASnS8EMzYGit30gPm4fICDez48X1e0Fusk4B9tc8WtmrP36WxNp5znullf	

- ... cualquier otra información que consideres importante que descubras (conseguir información extra a la especificada llevaría a la nota máxima)

He encontrado imágenes de conversaciones y de personas incriminatorias.

Adjunto las imágenes.





DroidPond



Hello World!

Storage use



RUNNING

ALL



Dialer
4.35MB



System UI
4.27MB



Google Play Games
4.11MB



Google Services Framework
3.40MB



<https://cyberhades.ams3>



```
ip:*:14195:0:99999:7:::
sync:*:14195:0:99999:7:::
shutdown:*:14195:0:99999:7:::
halt:*:14195:0:99999:7:::
mail:*:14195:0:99999:7:::
news:*:14195:0:99999:7:::
uucp:*:14195:0:99999:7:::
operator:*:14195:0:99999:7:::
games:*:14195:0:99999:7:::
gopher:*:14195:0:99999:7:::
ftp:*:14195:0:99999:7:::
nobody:*:14195:0:99999:7:::
rpm:!!:14195:0:99999:7:::
dbus:!!:14195:0:99999:7:::
avahi:!!:14195:0:99999:7:::
mailnull:!!:14195:0:99999:7:::
smb:!!:14195:0:99999:7:::
nscd:!!:14195:0:99999:7:::
vcsa:!!:14195:0:99999:7:::
rpc:!!:14195:0:99999:7:::
rpcuser:!!:14195:0:99999:7:::
```

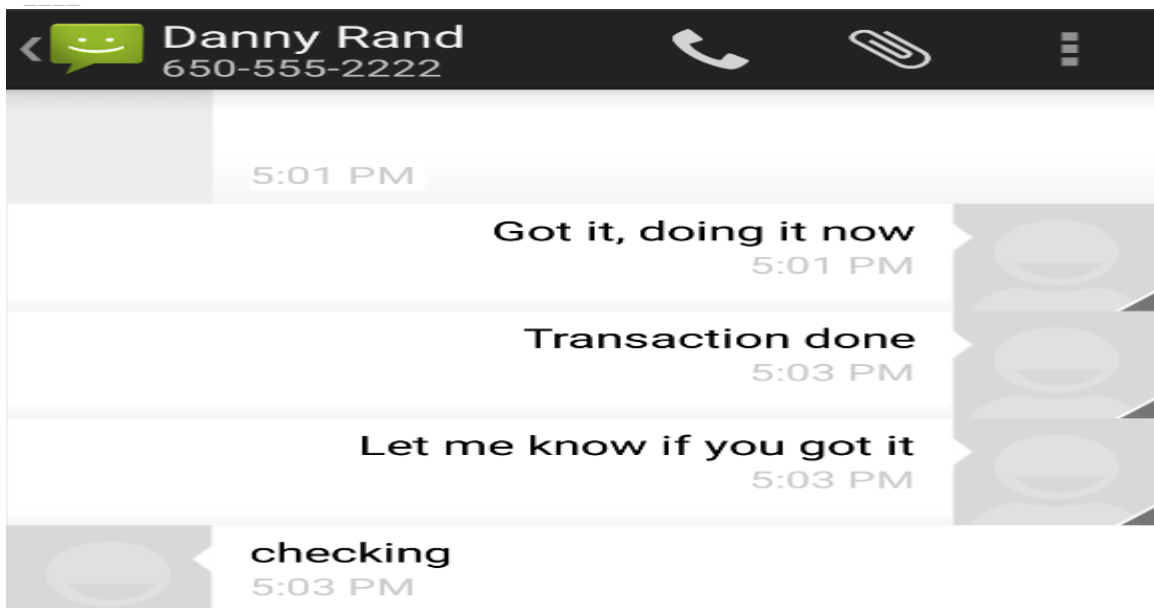


5:04 PM [View details](#)

<http://ultrarender.com/login>

username: rent20190099
password: ren7GPU!)(#*

You have a week, starting today.



Conlusiones.

MR X y Jessica necesitaban desbloquear el archivo Shadow que pertenece a una agencia de Estados Unidos de tres letras, Matt comparte el numero a MR X de Danny Rand el cual le alquila la granja de Bitcoin para llegar a realizar el trabajo por \$10000 a la semana. En conclusión, se MR X está jugando con fuego al llevar a cabo este trabajo.

Docker 1.

Crea una imagen Docker que levante contenedores que al ejecutarlos, convierta una imagen que pasamos como parámetro a imagen tipo ASCII art. El programa que podéis utilizar es jp2a pero cualquier otro es también válido (que realice la misma acción). El fichero generado debe de ser almacenado en un volumen llamado "asciiart" (si eliminar los otros que ya existan en el mismo volumen)

1- Apertura y construcción de Docker.

```
File Actions Edit View Help

(kali@kali)-[~]
$ docker --version

Docker version 20.10.25+dfsg1, build b82b9f3

(kali@kali)-[~]
$ sudo apt update
sudo apt install docker.io
sudo systemctl start docker
sudo systemctl enable docker

[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.8 MB]
Fetched 67.7 MB in 20s (3,318 kB/s)
14 packages can be upgraded. Run 'apt list --upgradable' to see them.
docker.io is already the newest version (20.10.25+dfsg1-3).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 14
Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker
```

2- Creación del directorio de trabajo.

Usa los comandos **mkdir ascii-art** y **cd ascii-art**

```
(kali@kali)-[~]
$ mkdir ascii-art

(kali@kali)-[~]
$ cd ascii-art
```

3- Creación del archivo Dockerfile.

Este archivo lo creamos con el comando **nano Dockerfile**

Utilizando las siguientes dependencias

FROM debian:latest

ENV DEBIAN_FRONTEND=noninteractive

**RUN apt-get update && apt-get install -y apt-utils && **
apt-get install -y jp2a bash && apt-get clean

VOLUME /asciiart

ENTRYPOINT ["/bin/bash"]



```
File Actions Edit View Help
GNU nano 8.1 Dockerfile *
FROM debian:latest

ENV DEBIAN_FRONTEND=noninteractive

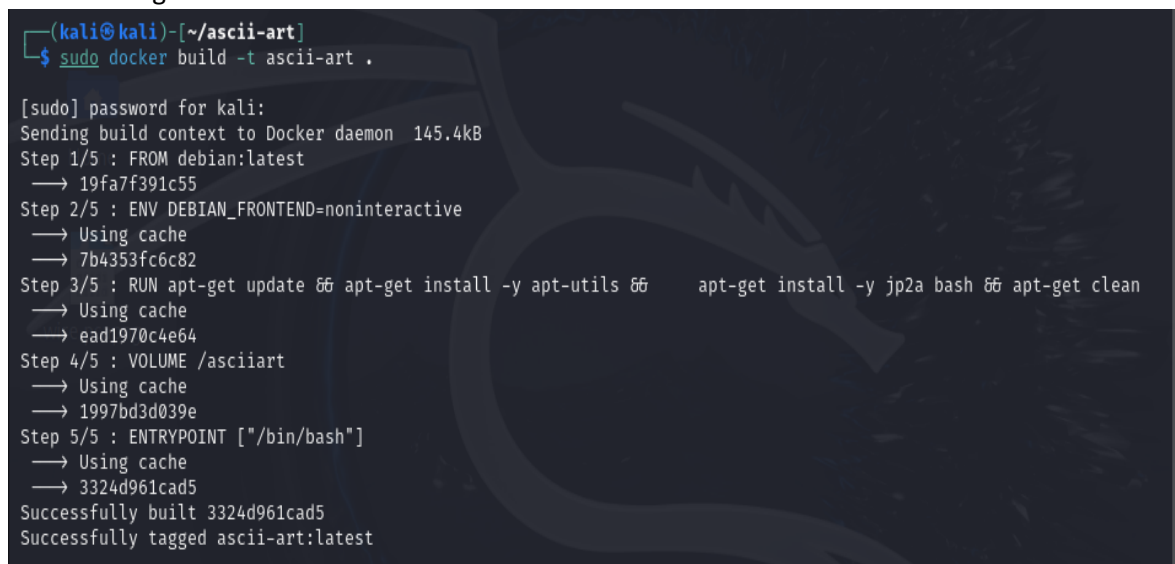
RUN apt-get update && apt-get install -y apt-utils && \
    apt-get install -y jp2a bash && apt-get clean

VOLUME /asciiart

ENTRYPOINT ["/bin/bash"]
█
```

4- Creación de la imagen Docker.

Usando el siguiente comando **sudo docker build -t ascii-art .**



```
(kali@kali)-[~/ascii-art]
$ sudo docker build -t ascii-art .

[sudo] password for kali:
Sending build context to Docker daemon 145.4kB
Step 1/5 : FROM debian:latest
-> 19fa7f391c55
Step 2/5 : ENV DEBIAN_FRONTEND=noninteractive
-> Using cache
-> 7b4353fc6c82
Step 3/5 : RUN apt-get update && apt-get install -y apt-utils && \
    apt-get install -y jp2a bash && apt-get clean
-> Using cache
-> ead1970c4e64
Step 4/5 : VOLUME /asciiart
-> Using cache
-> 1997bd3d039e
Step 5/5 : ENTRYPOINT ["/bin/bash"]
-> Using cache
-> 3324d961cad5
Successfully built 3324d961cad5
Successfully tagged ascii-art:latest
```


2. Crea una arquitectura WordPress + MySQL con persistencia de datos (volumen) primero con DockerFile y luego con DockerCompose.

1- Actualización e instalación de Docker compose.

```
(kali@kali)-[~]
$ sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
14 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali@kali)-[~]
$ sudo apt install docker-compose
Installing:
  docker-compose

Installing dependencies:
  python3-compose python3-docker python3-dockerpty python3-texttable

Summary:
  Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 14
  Download size: 269 kB
  Space needed: 1,237 kB / 58.6 GB available
Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 python3-docker all 7.1.0-1 [89.7 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 python3-dockerpty all 0.4.1-5 [11.2 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 python3-compose all 1.29.2-6.3 [112 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 docker-compose all 1.29.2-6.3 [44.0 kB]
Get:3 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 python3-texttable all 1.7.0-1 [12.0 kB]
Fetched 269 kB in 1s (192 kB/s)
Selecting previously unselected package python3-docker.
(Reading database ... 407787 files and directories currently installed.)
Preparing to unpack .../python3-docker_7.1.0-1_all.deb ...
Unpacking python3-docker (7.1.0-1) ...
Selecting previously unselected package python3-dockerpty.
Preparing to unpack .../python3-dockerpty_0.4.1-5_all.deb ...
Unpacking python3-dockerpty (0.4.1-5) ...
Selecting previously unselected package python3-texttable.
Preparing to unpack .../python3-texttable_1.7.0-1_all.deb ...
Unpacking python3-texttable (1.7.0-1) ...
Selecting previously unselected package python3-compose.
Preparing to unpack .../python3-compose_1.29.2-6.3_all.deb ...
Unpacking python3-compose (1.29.2-6.3) ...
Selecting previously unselected package docker-compose.
Preparing to unpack .../docker-compose_1.29.2-6.3_all.deb ...
Unpacking docker-compose (1.29.2-6.3) ...
Setting up python3-texttable (1.7.0-1) ...
Setting up python3-docker (7.1.0-1) ...
Setting up python3-dockerpty (0.4.1-5) ...
Setting up python3-compose (1.29.2-6.3) ...
Setting up docker-compose (1.29.2-6.3) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for man-db (2.12.1-3) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.
```

2- Creación del Dockerfile para MySQL.

```
File Actions Edit View Help

(kali@kali)-[~]
$ mkdir mysql

(kali@kali)-[~]
$ cd mysql
```

3- Creación del archivo Dockerfile para MySQL.

The image shows a Kali Linux terminal window. At the top, the terminal title is "kali@kali: ~". The main content is a Dockerfile being edited in nano 8.1. The Dockerfile content is as follows:

```
GNU nano 8.1 Dockerfile *
FROM mysql:5.7

ENV MYSQL_DATABASE=wordpress
ENV MYSQL_USER=wp_user
ENV MYSQL_PASSWORD=secret
ENV MYSQL_ROOT_PASSWORD=root_secret

VOLUME /var/lib/mysql
EXPOSE 3306
```

Below the Dockerfile content, the WordPress installation language selection screen is visible. It lists various languages, with "English (United States)" selected. Other visible languages include Afrikaans, العربية, Azərbaycan dili, Беларуская мова, Български, বাংলা, Bosanski, Català, and Cebuano. A "Continue" button is at the bottom right of the language selection box. At the bottom of the terminal, a status bar shows keyboard shortcuts: ^G Help, ^O Write Out, ^F Where Is, ^K Cut, ^T Execute, ^C Location, ^M-U Undo, ^X Exit, ^R Read File, ^\ Replace, ^U Paste, ^J Justify, ^_/ Go To Line, and ^M-E Redo.

4- Construcción de la imagen de MySQL.

```
kali@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~/mysql]─┐  
$ sudo nano Dockerfile  
└─(kali@kali)-[~/mysql]─┐  
$ sudo docker build -t custom-mysql .  
  
Sending build context to Docker daemon 3.072kB  
Step 1/7 : FROM mysql:5.7  
5.7: Pulling from library/mysql  
20e4dcae4c69: Pull complete  
1c56c3d4ce74: Pull complete  
e9f03a1c24ce: Pull complete  
68c3898c2015: Pull complete  
6b95a940e7b6: Pull complete  
90986bb8de6e: Pull complete  
ae71319cb779: Pull complete  
ffc89e9dfd88: Pull complete  
43d05e938198: Pull complete  
064b2d298fba: Pull complete  
df9a4d85569b: Pull complete  
Digest: sha256:4bc6bc963e6d8443453676cae56536f4b8156d78bae03c0145cbe47c2aad73bb  
Status: Downloaded newer image for mysql:5.7  
→ 5107333e08a8  
Step 2/7 : ENV MYSQL_DATABASE=wordpress  
→ Running in ce6fad7bd0ec  
Removing intermediate container ce6fad7bd0ec  
→ ce2ebbd4d17f  
Step 3/7 : ENV MYSQL_USER=wp_user  
→ Running in 4b2922f49a53  
Removing intermediate container 4b2922f49a53  
→ 7510e6c1aa98  
Step 4/7 : ENV MYSQL_PASSWORD=secret  
→ Running in 9684d8d19bf8  
Removing intermediate container 9684d8d19bf8  
→ b8058fa85725  
Step 5/7 : ENV MYSQL_ROOT_PASSWORD=root_secret  
→ Running in 96eda41e479d  
Removing intermediate container 96eda41e479d  
→ 0a32d14641c3  
Step 6/7 : VOLUME /var/lib/mysql  
→ Running in 925b8fcfe7ec  
Removing intermediate container 925b8fcfe7ec  
→ aafc1c52b432  
Step 7/7 : EXPOSE 3306  
→ Running in 0e081c10ca74  
Removing intermediate container 0e081c10ca74  
→ af8b81c7935d  
Successfully built af8b81c7935d  
Successfully tagged custom-mysql:latest  
  
└─(kali@kali)-[~/mysql]  
$ cd ..
```

Docker file para wordpress.

1- Volver al directorio.

Vuelvo al directorio raíz para crear el directorio de Wordpress con los comandos

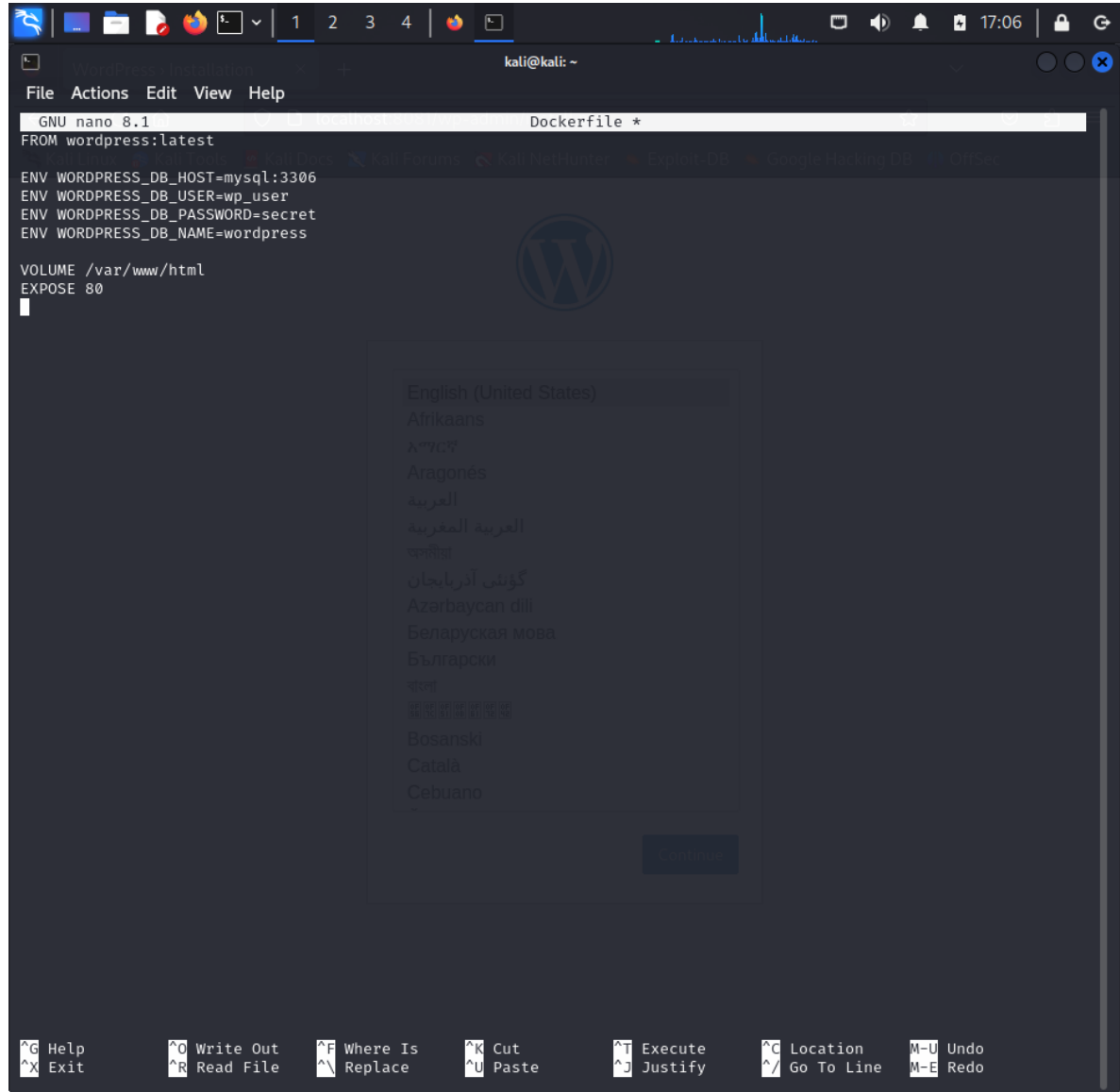
cd ..

mkdir wordpress

cd wordpress

```
└─(kali@kali)-[~/mysql]  
$ cd ..  
  
└─(kali@kali)-[~]  
$ mkdir wordpress  
  
└─(kali@kali)-[~]  
$ cd wordpress
```

- 2- Creación del archivo Dockerfile para Wordpress.
Ejecuto el comando nano Dockerfile.



```
GNU nano 8.1 Dockerfile *
FROM wordpress:latest

ENV WORDPRESS_DB_HOST=mysql:3306
ENV WORDPRESS_DB_USER=wp_user
ENV WORDPRESS_DB_PASSWORD=secret
ENV WORDPRESS_DB_NAME=wordpress

VOLUME /var/www/html
EXPOSE 80
```

English (United States)
Afrikaans
አማርኛ
Aragonés
العربية
العربية المغربية
অসমীয়া
ગુજરાતી
Azərbaycan dili
Беларуская мова
Български
বাংলা
Босански
Català
Cebuano

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo

3- Creación de la imagen de Wordpress.

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali] (~/wordpress)  
$ sudo docker build -t custom-wordpress  
"docker build" requires exactly 1 argument.  
See 'docker build --help'.  
  
Usage: docker build [OPTIONS] PATH | URL | -  
  
Build an image from a Dockerfile  
  
[kali@kali] (~/wordpress)  
$ sudo docker build -t custom-wordpress .  
  
Sending build context to Docker daemon 2.648kB  
Step 1/7 : FROM wordpress:latest  
latest: pulling from library/wordpress  
e4ff8799edd: Pull complete  
eb65c9579cf: Pull complete  
73f9b0bf245b: Pull complete  
629db81c17f: Pull complete  
364fd86af72d: Pull complete  
de55dbd5d228: Pull complete  
180e8548b09: Pull complete  
8894b87cf8a: Pull complete  
67cfe838099: Pull complete  
69222b06ade: Pull complete  
3992a4a5ade: Pull complete  
126a489d1344: Pull complete  
a1fee752f3f9: Pull complete  
73d0a15d5f: Pull complete  
56bbd5f0138: Pull complete  
2e44139c2607: Pull complete  
98d6faf3fa7: Pull complete  
4f0b8935c5d: Pull complete  
1b7cf87833c: Pull complete  
b9a329a4a02d: Pull complete  
85da746128f: Pull complete  
Digest: sha256:c829a137becb34fc1cd198b12a82b91aae918524daf4e3b1b783d79a618  
Status: Downloaded newer image for wordpress:latest  
→ e826d932896c  
Step 2/7 : ENV WORDPRESS_DB_HOST=mysql:3306  
→ Running in 44b71cf7646f  
Removing intermediate container 44b71cf7646f  
→ 9eab1ef54fc  
Step 3/7 : ENV WORDPRESS_DB_USER=wp_user  
→ Running in f19fa59fb2ab  
Removing intermediate container f19fa59fb2ab  
→ 2c9353a5346  
Step 4/7 : ENV WORDPRESS_DB_PASSWORD=secret  
→ Running in 9e22cbff0331  
Removing intermediate container 9e22cbff0331  
→ 91c417bf081e  
Step 5/7 : ENV WORDPRESS_DB_NAME=wordpress
```

4- Creamos una red de dockers.

Creamos una red personalizada para que los contenedores de MySQL y WordPress se puedan comunicar entre sí y ejecutamos los contenedores.

```
kali@kali: ~  
File Actions Edit View Help  
Step 7/7 : EXPOSE 80  
→ Running in 381ef693afc  
Removing intermediate container 381ef693afc  
→ e247c3563b79  
Successfully built e247c3563b79  
Successfully tagged custom-wordpress:latest  
  
[kali@kali] (~/wordpress)  
$ sudo docker network create wp_network  
3b3708eada57f8506e3098a165d619048d20b9f3bd13731a70b0eaf520ff01909  
  
[kali@kali] (~/wordpress)  
$ sudo docker run -d --name mysql-container --network wp_network -v mysql_data:/var/lib/mysql custom-mysql  
f7aa2518e4a9eb0ba95046f96ae5c116971e19b2e87d49470bf24c535aba223  
  
[kali@kali] (~/wordpress)  
$ sudo docker run -d --name wordpress-container --network wp_network -p 8080:80 -v wordpress_data:/var/www/html c  
ustom-wordpress  
41a3852e413f018f79b0ff0e3506eff21372b223a06f2c62db0fc0875ba0d
```

5- Creación del archivo Dockercompose.

```

GNU nano 8.1 docker-compose.yml
Version: '3.7'

services:
  mysql:
    image: mysql:5.7
    volumes:
      - mysql_data:/var/lib/mysql
    environment:
      MYSQL_DATABASE: wordpress
      MYSQL_USER: wp_user
      MYSQL_PASSWORD: secret
      MYSQL_ROOT_PASSWORD: root_secret
    networks:
      - wp_network

  wordpress:
    image: wordpress:latest
    ports:
      - "8081:80"
    volumes:
      - wordpress_data:/var/www/html
    environment:
      WORDPRESS_DB_HOST: mysql:3306
      WORDPRESS_DB_USER: wp_user
      WORDPRESS_DB_PASSWORD: secret
      WORDPRESS_DB_NAME: wordpress
    networks:
      - wp_network

volumes:
  mysql_data:
  wordpress_data:

networks:
  wp_network:
  
```

English (United States)
 Afrikaans
 አማርኛ
 Aragonés
 العربية
 العربية المغربية
 বাংলা
 گۆنئی آذربایجان
 Azərbaycan dili
 Беларуская мова
 Български
 বাংলা
 বাংলা
 Bosanski
 Català
 Cebuano

[Read 36 lines]

^G Help ^O Write Out ^F Where Is ^K Cut Execute ^C Location M-U Undo
 ^X Exit ^R Read File ^\ Replace ^U Paste Justify ^_ Go To Line M-E Redo

6- Levantamiento y verificación de que los contenedores compose esten correctamente.

```

(kali@kali)-[~]
$ sudo docker-compose up -d
Recreating kali_wordpress_1 ...
Recreating kali_wordpress_1 ... done

(kali@kali)-[~]
$ sudo docker ps

```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
a0a0976c6463	wordpress:latest	"docker-entrypoint.s..."	41 seconds ago	Up 39 seconds	0.0.0.0:8081→80/tcp, :
4f8912767aae	mysql:5.7	"docker-entrypoint.s..."	2 minutes ago	Up 2 minutes	3306/tcp, 33060/tcp
4143852e413f	custom-wordpress	"docker-entrypoint.s..."	6 minutes ago	Up 6 minutes	0.0.0.0:8080→80/tcp, :
f7aa2518e4a0	custom-mysql	"docker-entrypoint.s..."	6 minutes ago	Up 6 minutes	3306/tcp, 33060/tcp