**Operation:** Digital Forensic Investigation

[1. Overview of the Case 3](#_Toc110416764)

[1.1 Required Findings 3](#_Toc110416765)

[1.2 Acceptable internet use policy for UBB 3](#_Toc110416766)

[1.3 Unacceptable behavior 3](#_Toc110416767)

[2. Literature review 4](#_Toc110416769)

[2.1 Critical Discus 4](#_Toc110416770)

[2.2 References 5](#_Toc110416770)

[3. Digital forensics analysis 6](#_Toc110416775)

[3.1 the Evidence File is opened by autopsy 6](#_Toc110416776)

[3.2 Hash value of the Evidence File 6](#_Toc110416777)

[3.3 analysis process 7](#_Toc110416777)

[4. the toolkit 19](#_Toc110416778)

# 1. Overview of the Case

## 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 .

## 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.

## 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.

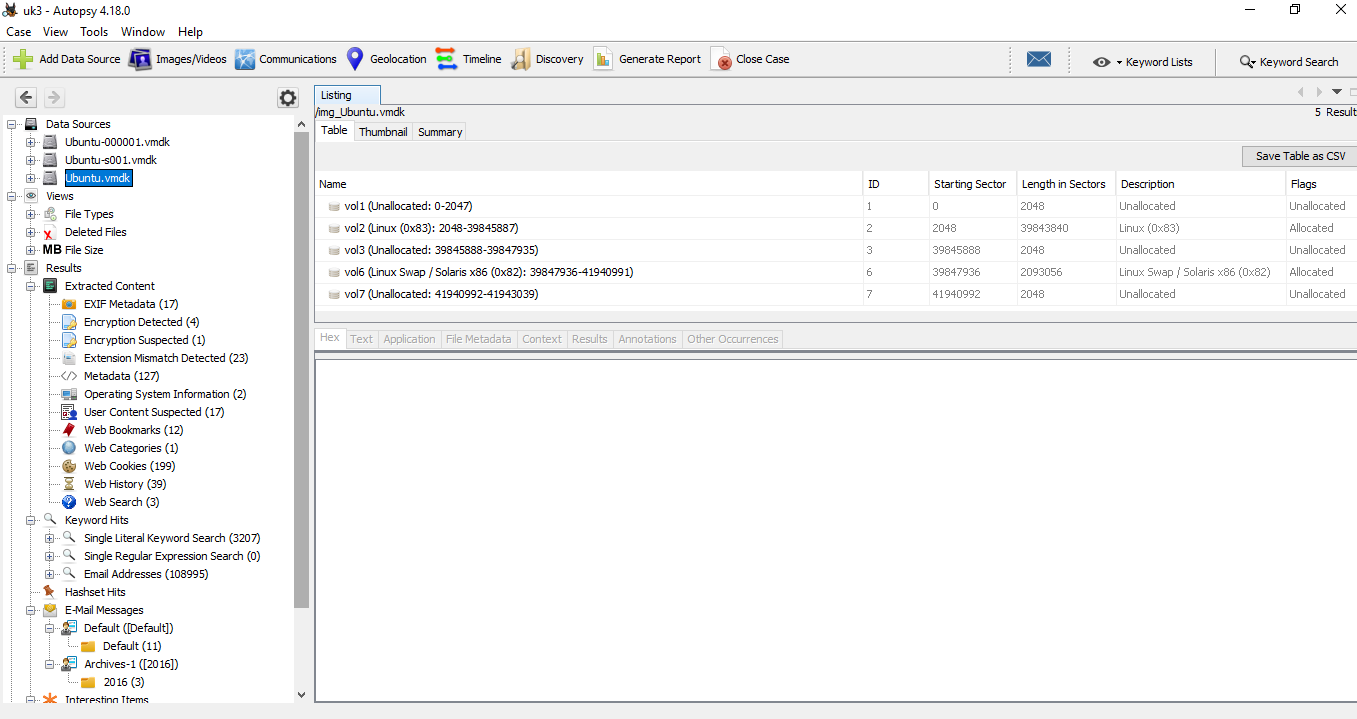
Casey, E. (2011). Digital evidence and computer crime: forensic science, computers and the Internet. Academic Press.

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

# 3. Digital Forensics Analysis

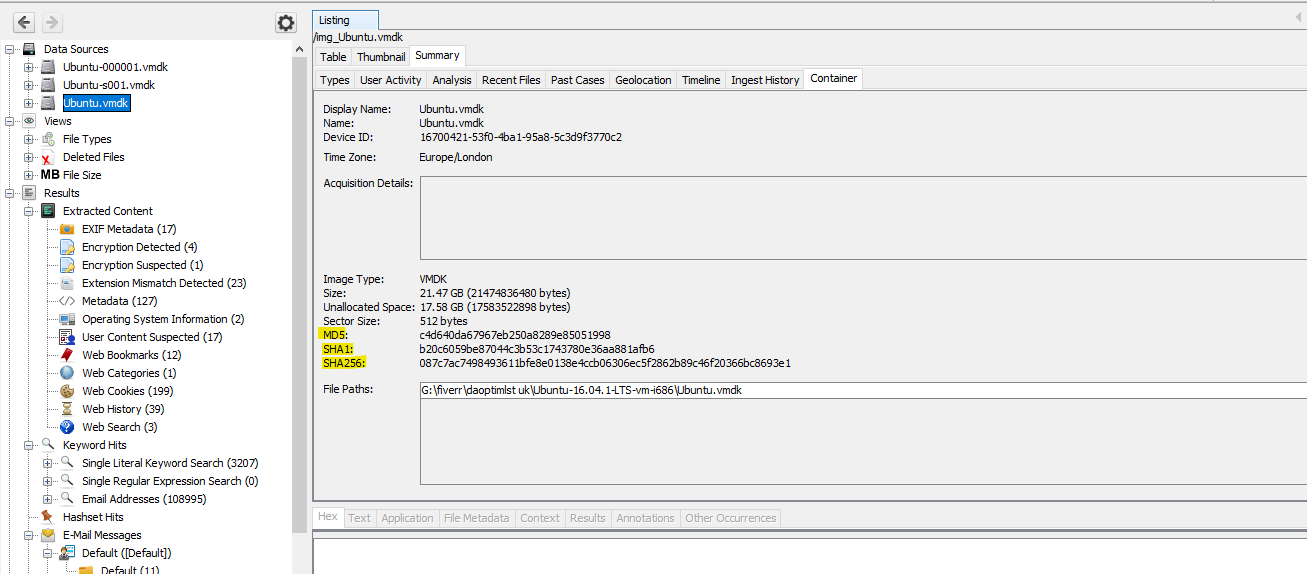
## 3.1 The Evidence File is Opened by Autopsy

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



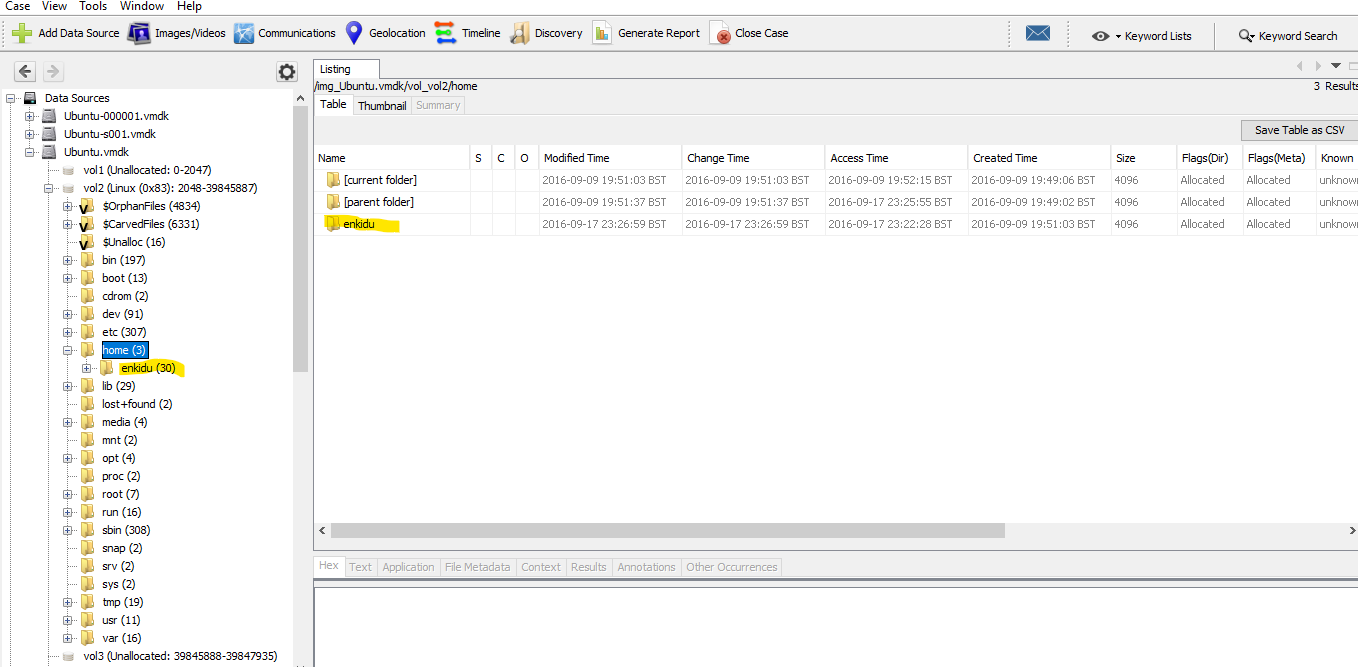
## 3.2 Hash value of the Evidence File

**And the hash value of this VM:**



## 3.3 Analysis Process

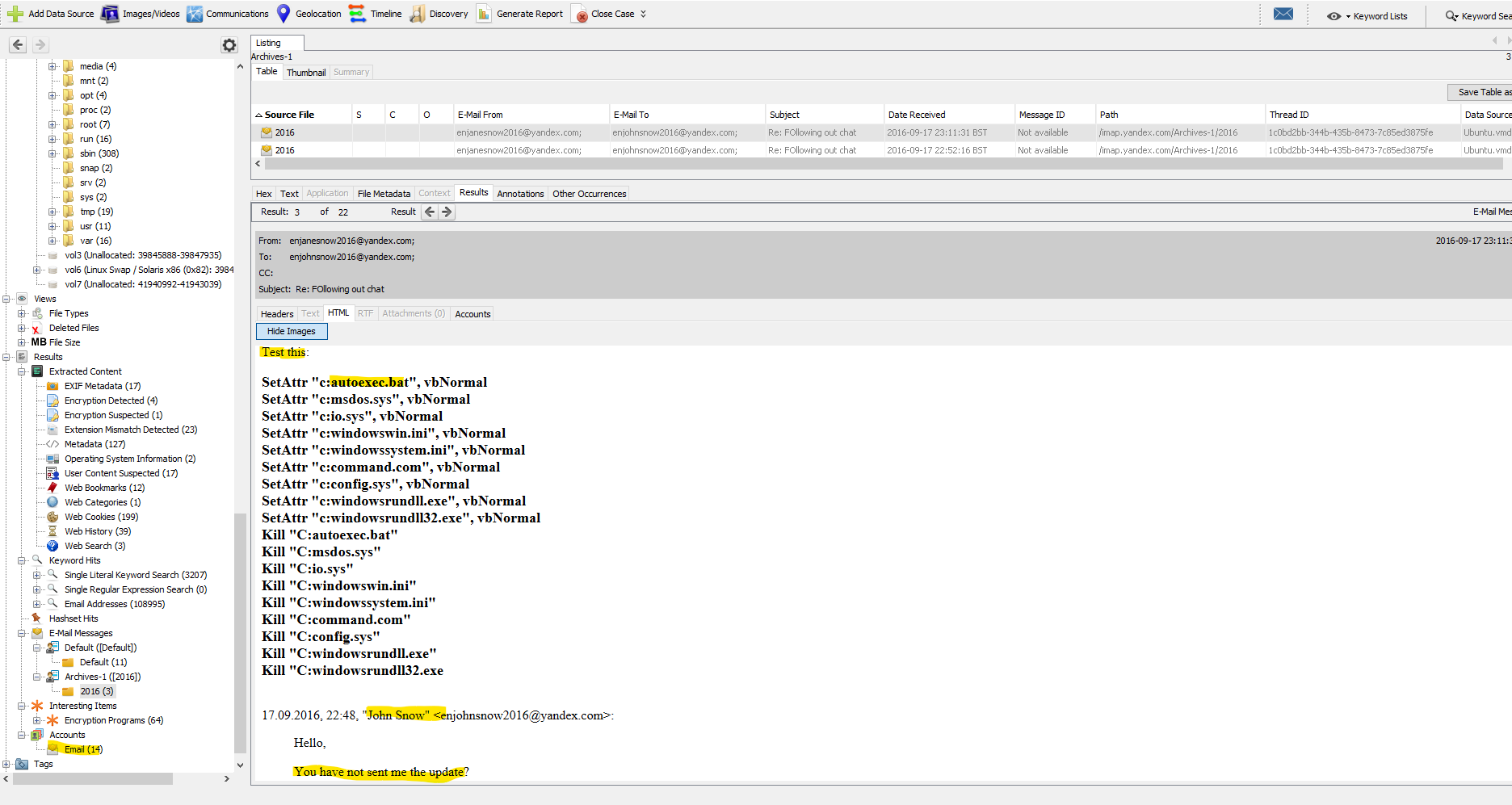
On **/home** directory there have a user and the username is **“enkidu”**.



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

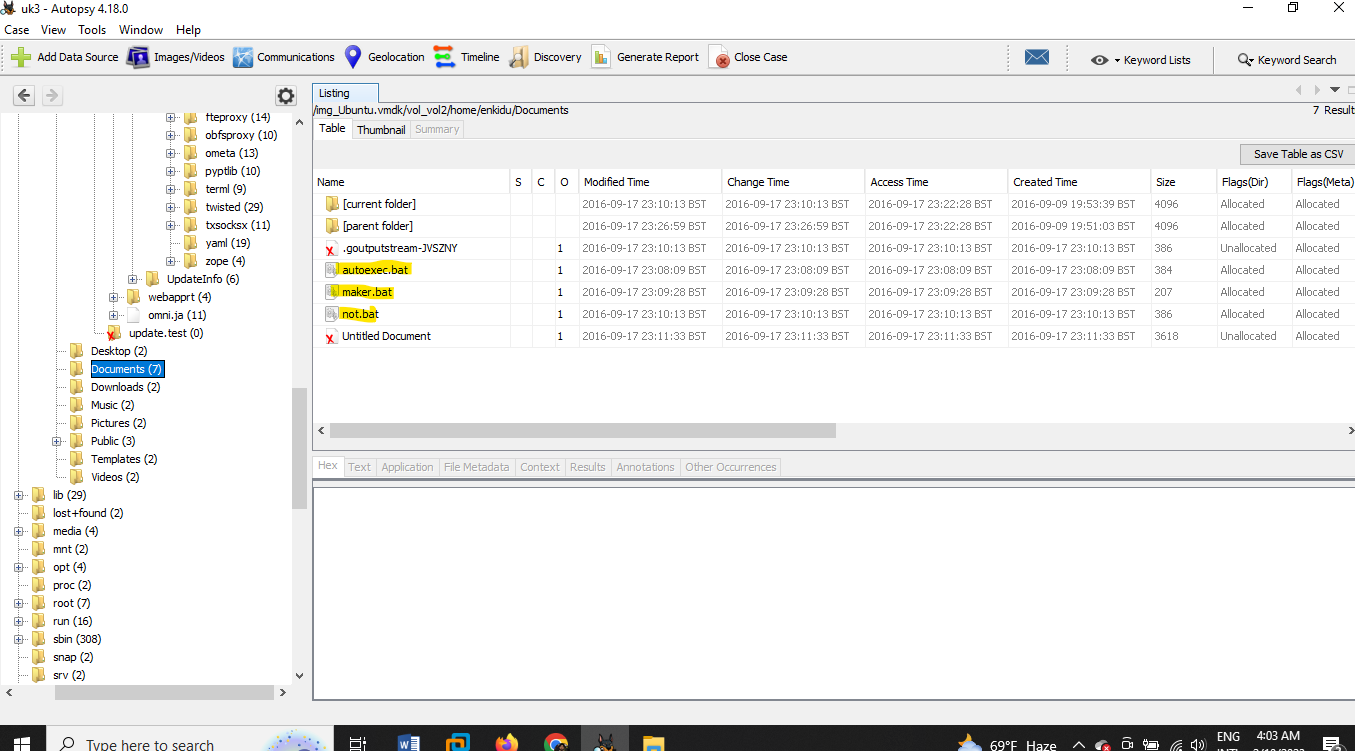
Email address: [enjohnsnow2016@gmail.com](mailto:enjohnsnow2016@gmail.com)

**1st mail:**

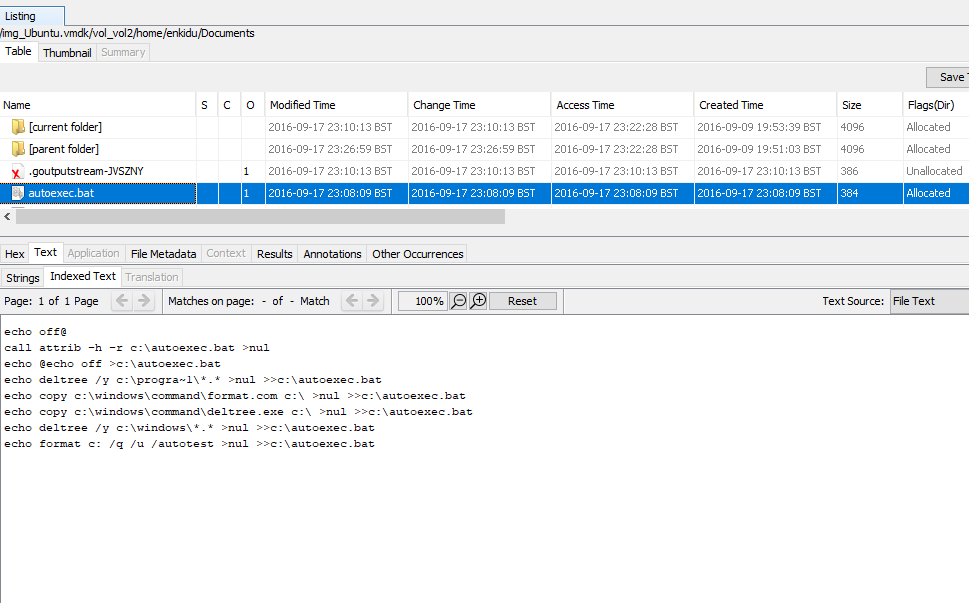


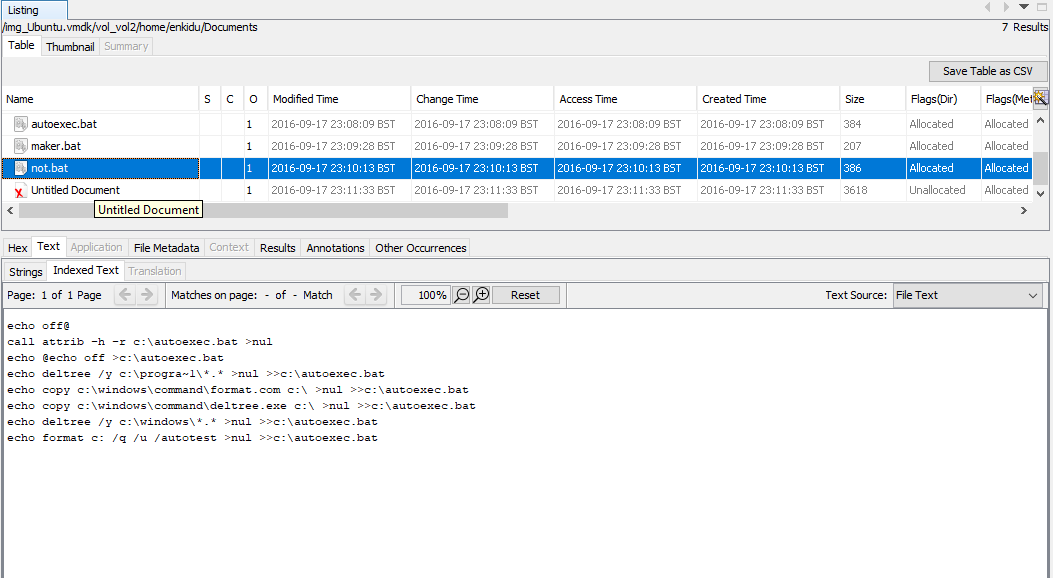
Here, it is clear that the suspect John Snow sent the local user some instructions for running the **"autoexec.bat"** file.

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



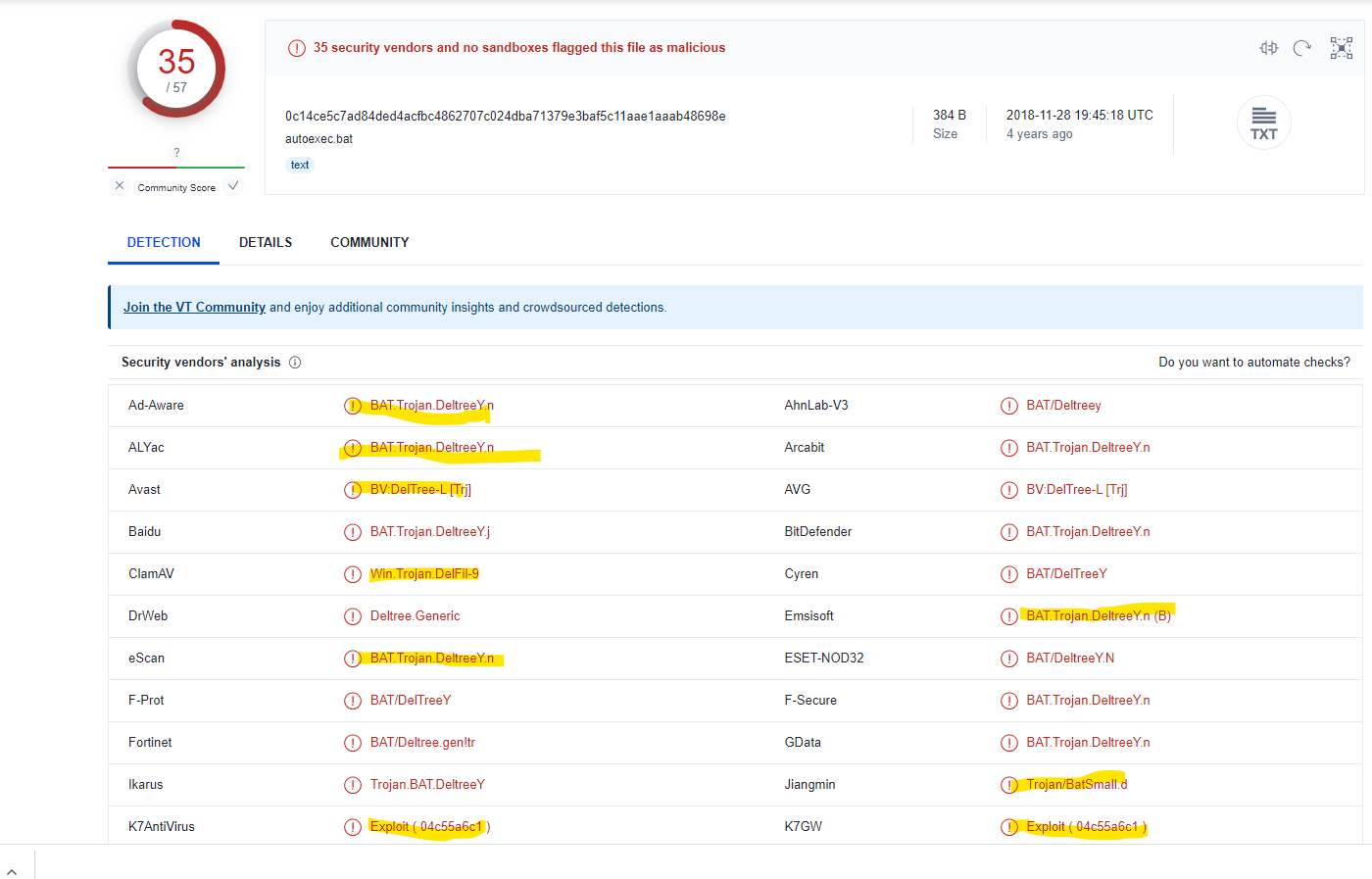
**Three bat files are displayed here:** **"autoexec.bat"**, **"maker.bat"** and **"not.bat".** The **autoexec.bat** and **not.bat** scripts are identical.

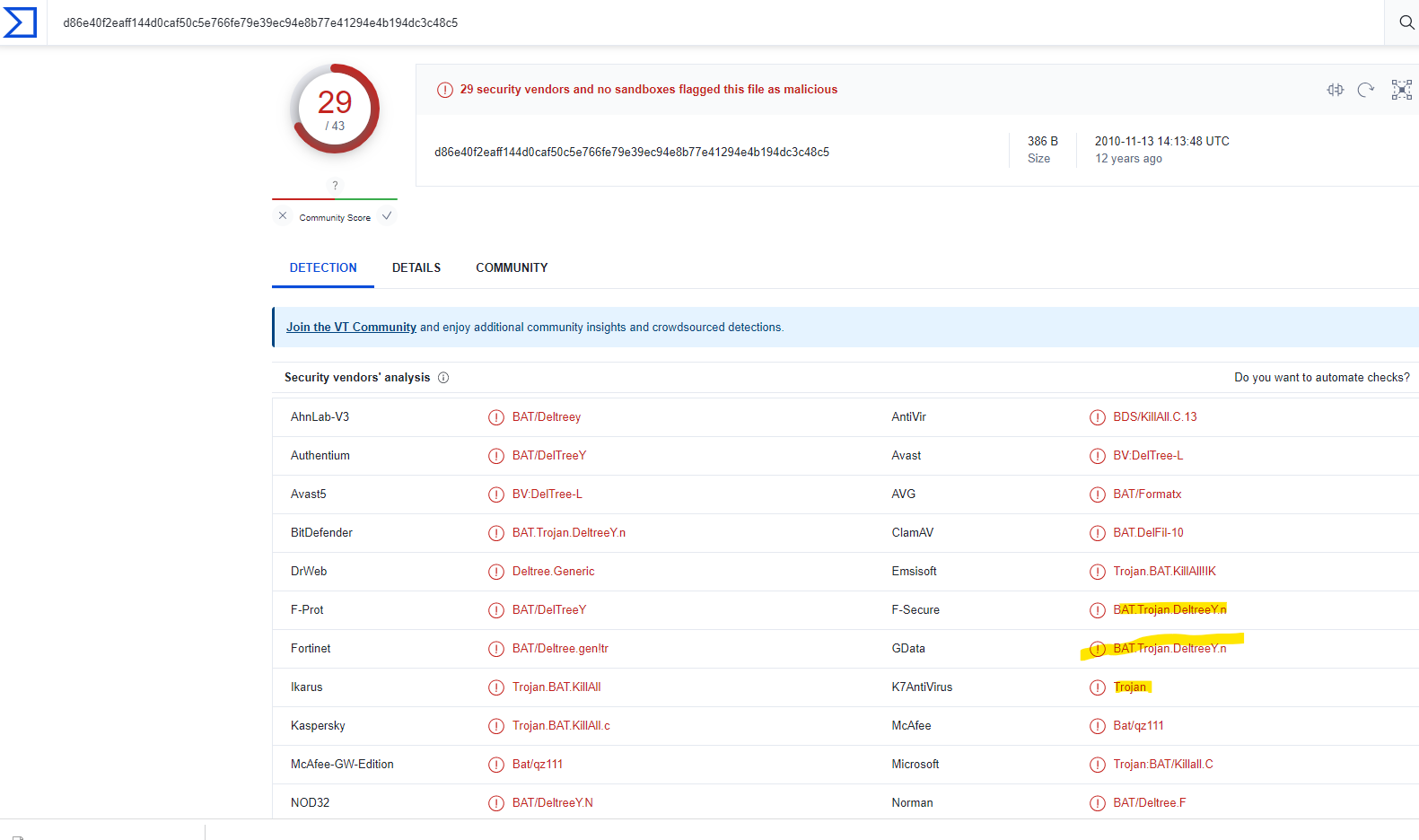




It is guaranteed that these files are run automatically after clicking them thanks to our analysis of the scripts. Furthermore, it will undermine the system.

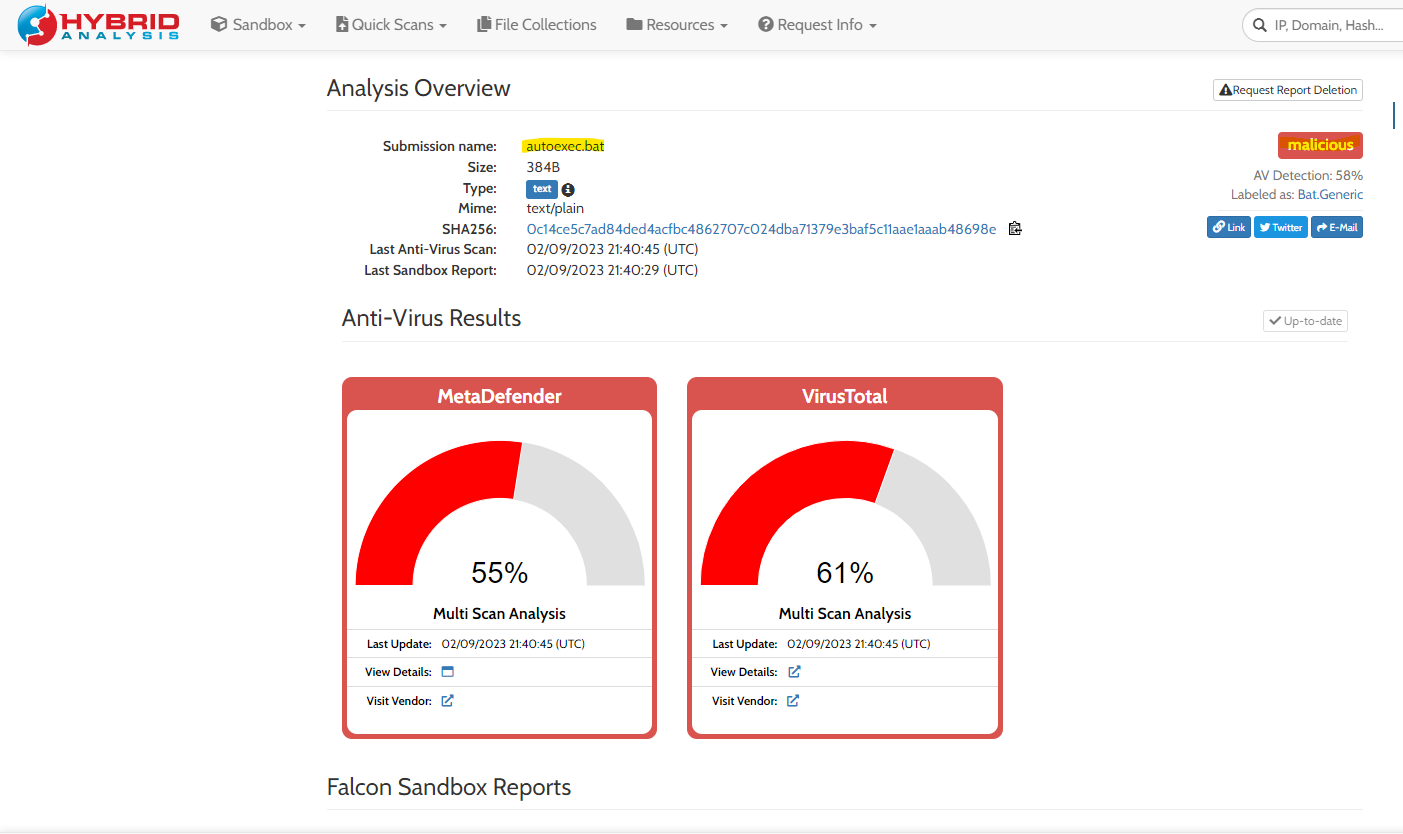
Here, export these two bat files and do a virus check using the website **"Virustotal".**

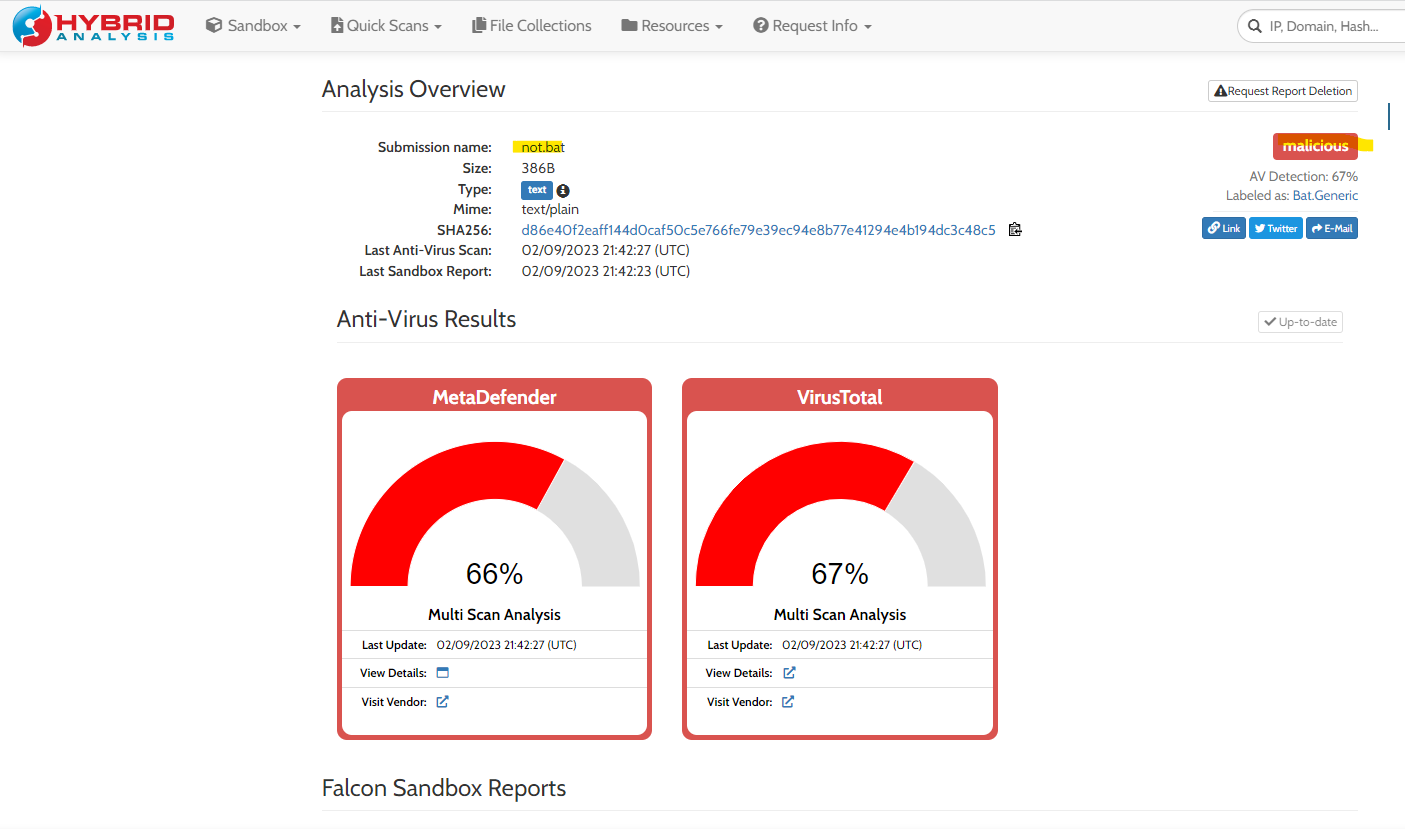




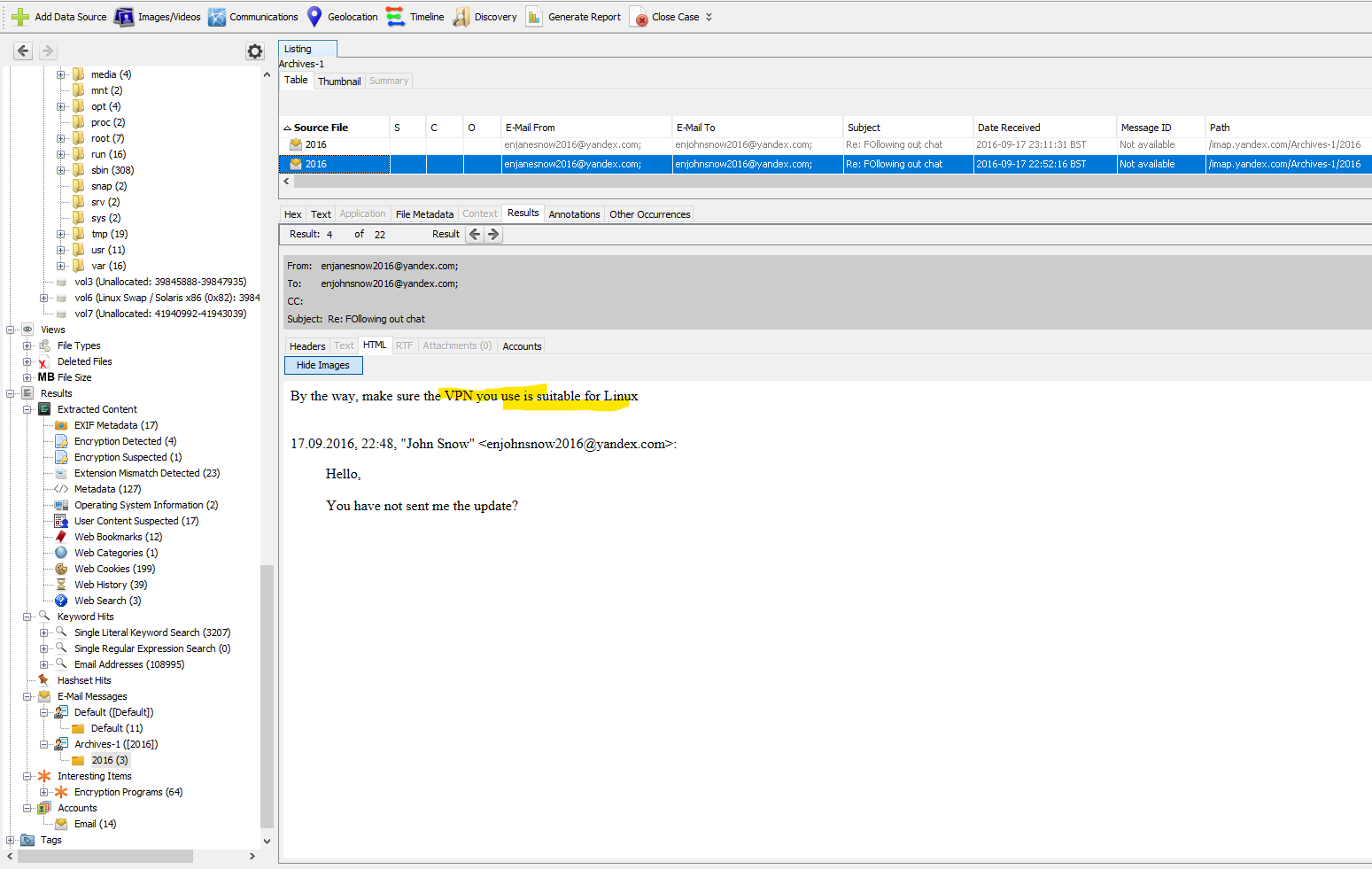
The files **"autoexec.bat"** and **"not.bat"** are **"Trojan"** according to the virus total tool.

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



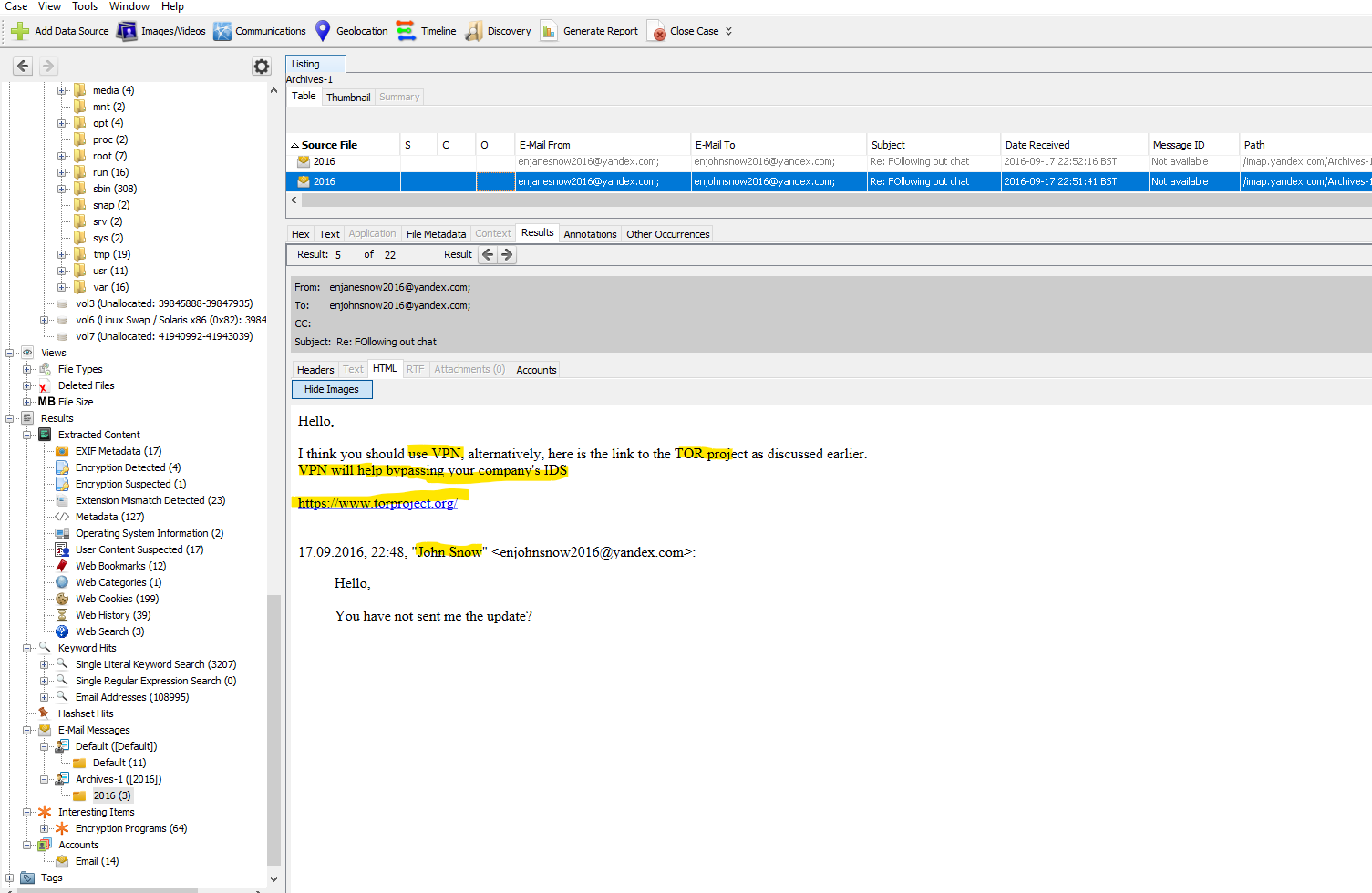


**2nd mail:**



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

**3rd mail:**

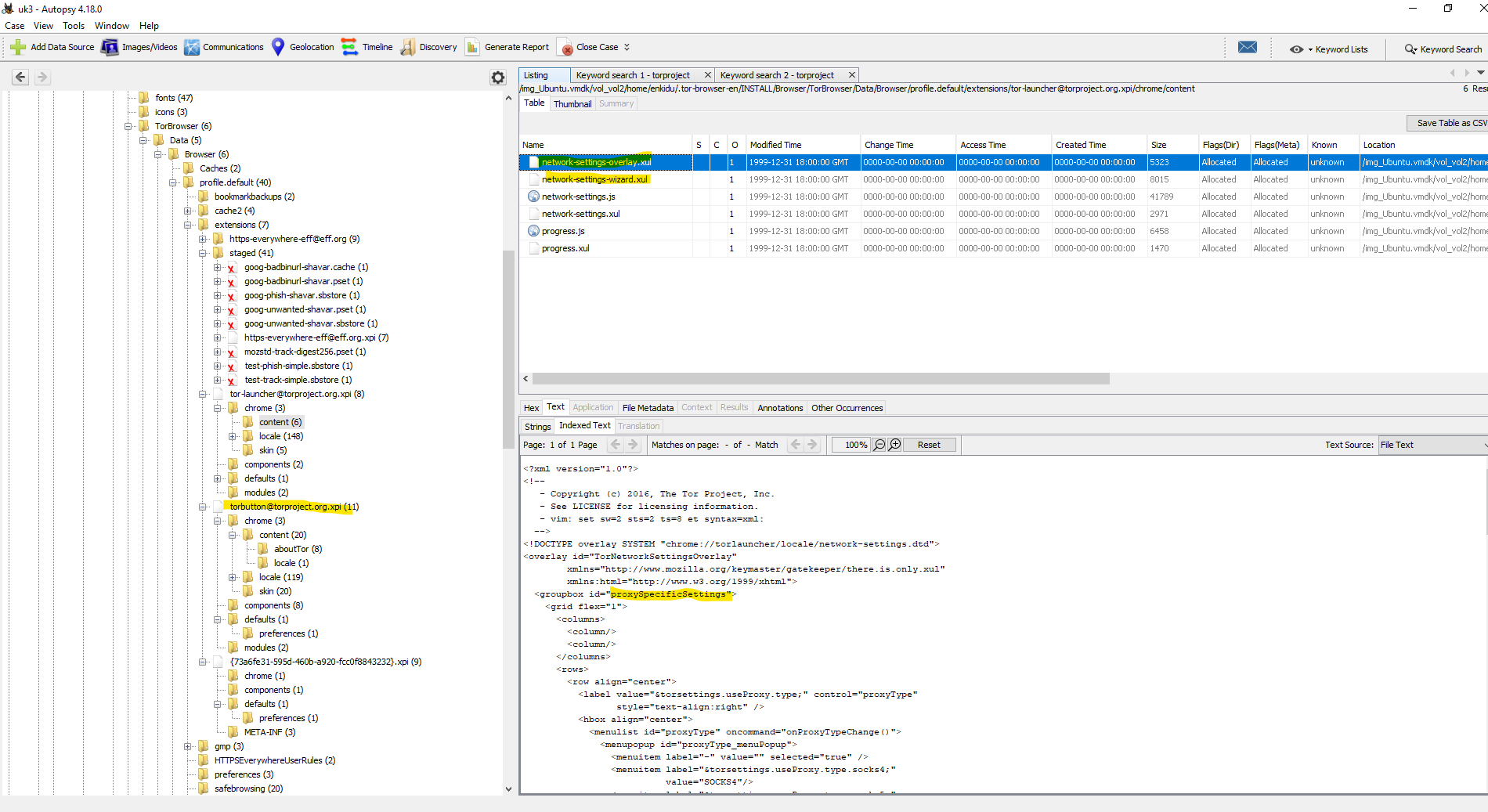


Here, confirm that "John Snow" has instructed you in this email to use a VPN to get around the **company's IDS.**

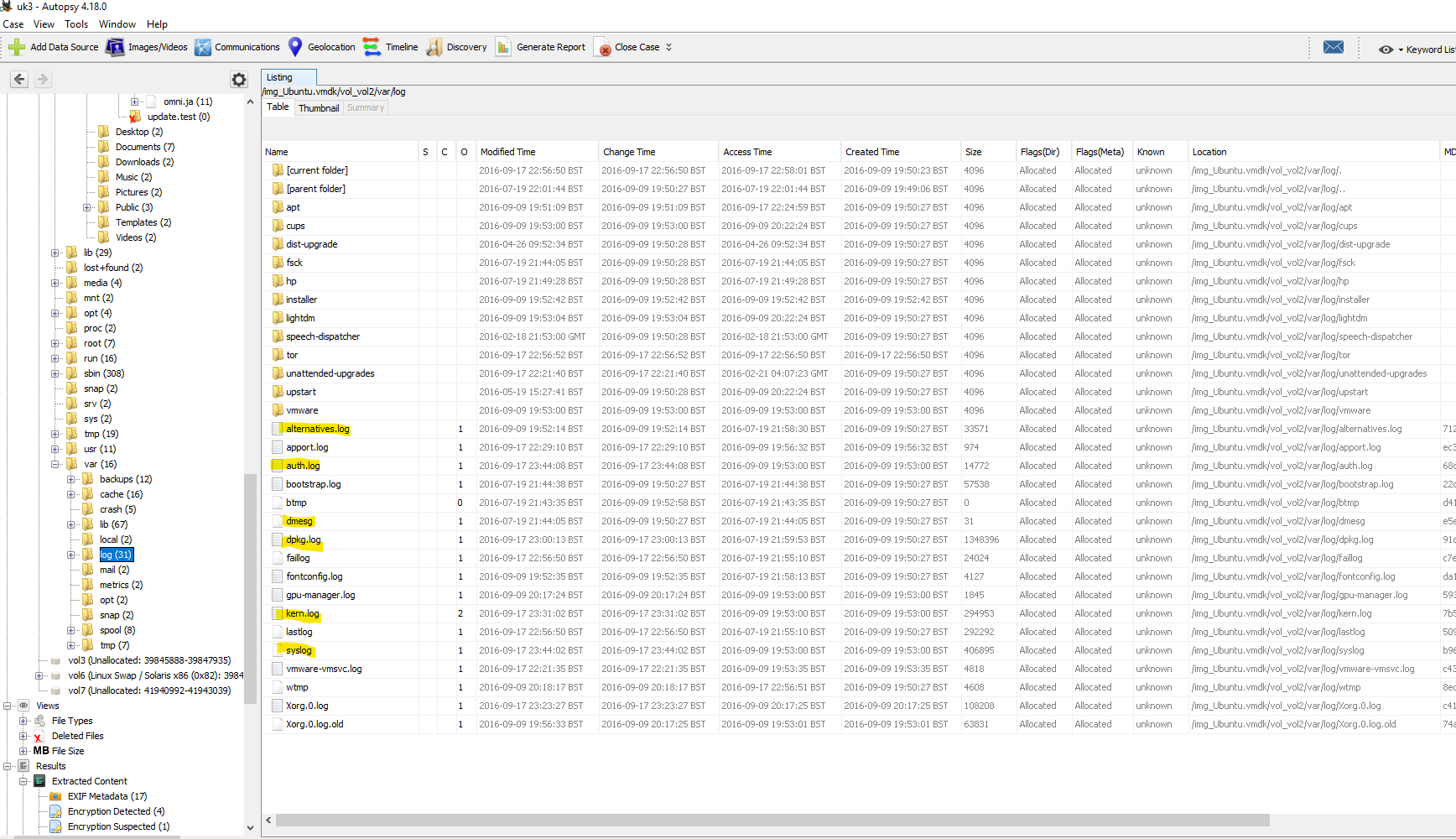
Here, the suspect also makes reference to the **"TOR project"** which is a VPN substitute. Thus, by starting this project, the local user is also able to go through the **firewall and IDS** of the corporation.

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**](mailto:tor-launcher@torproject.org)**.xpi/**

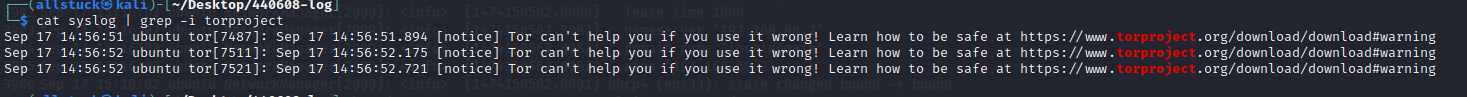


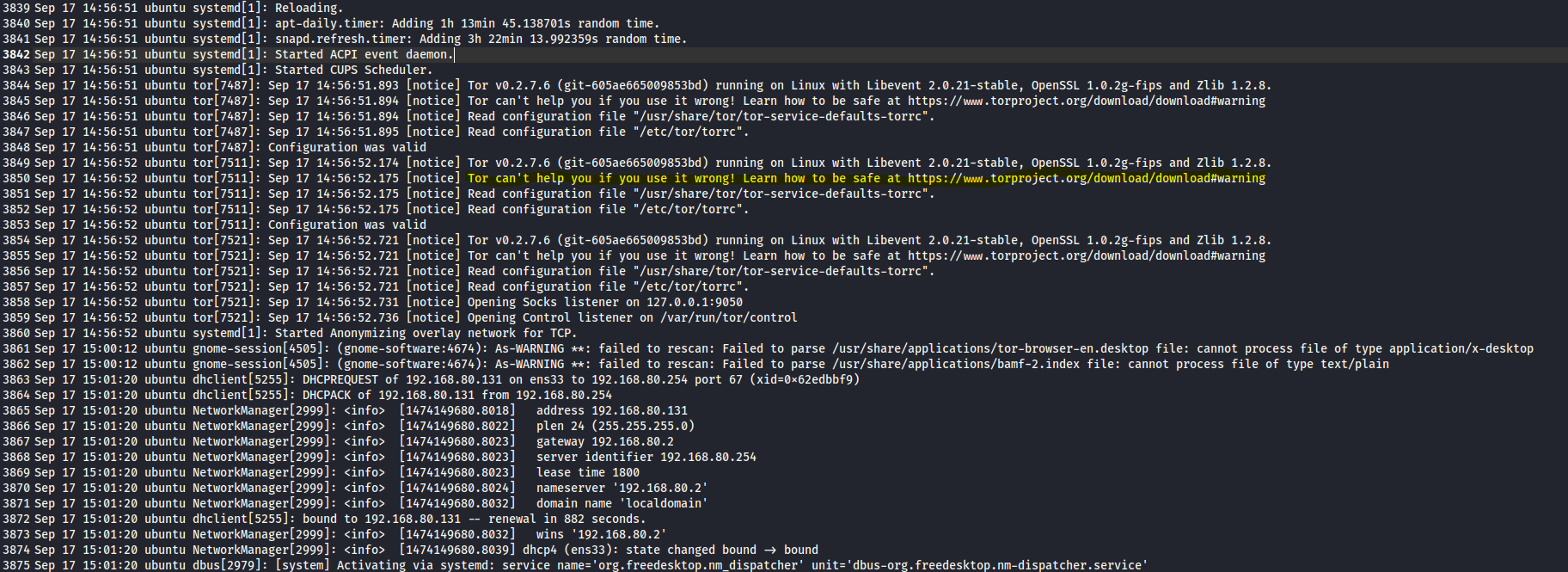
There have some important log files in **/var/log/** directory.

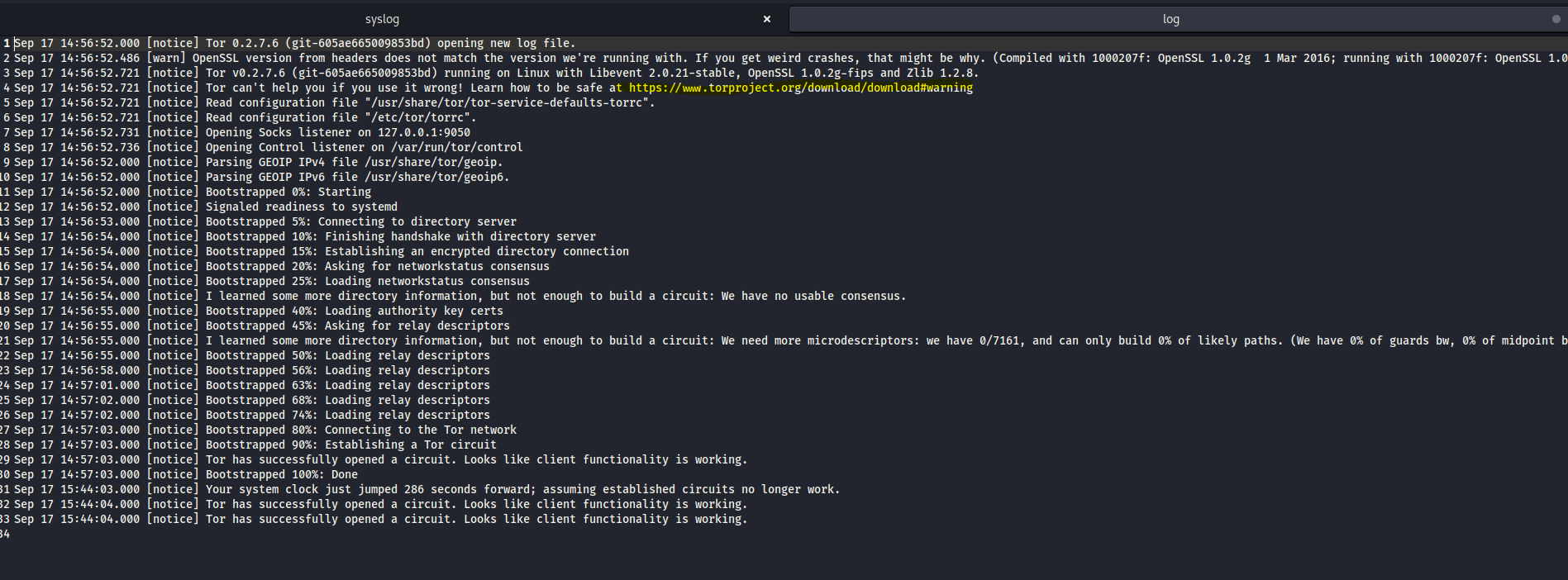


After exporting all log files and after analyzing all logs, find proof of launching the tor project.

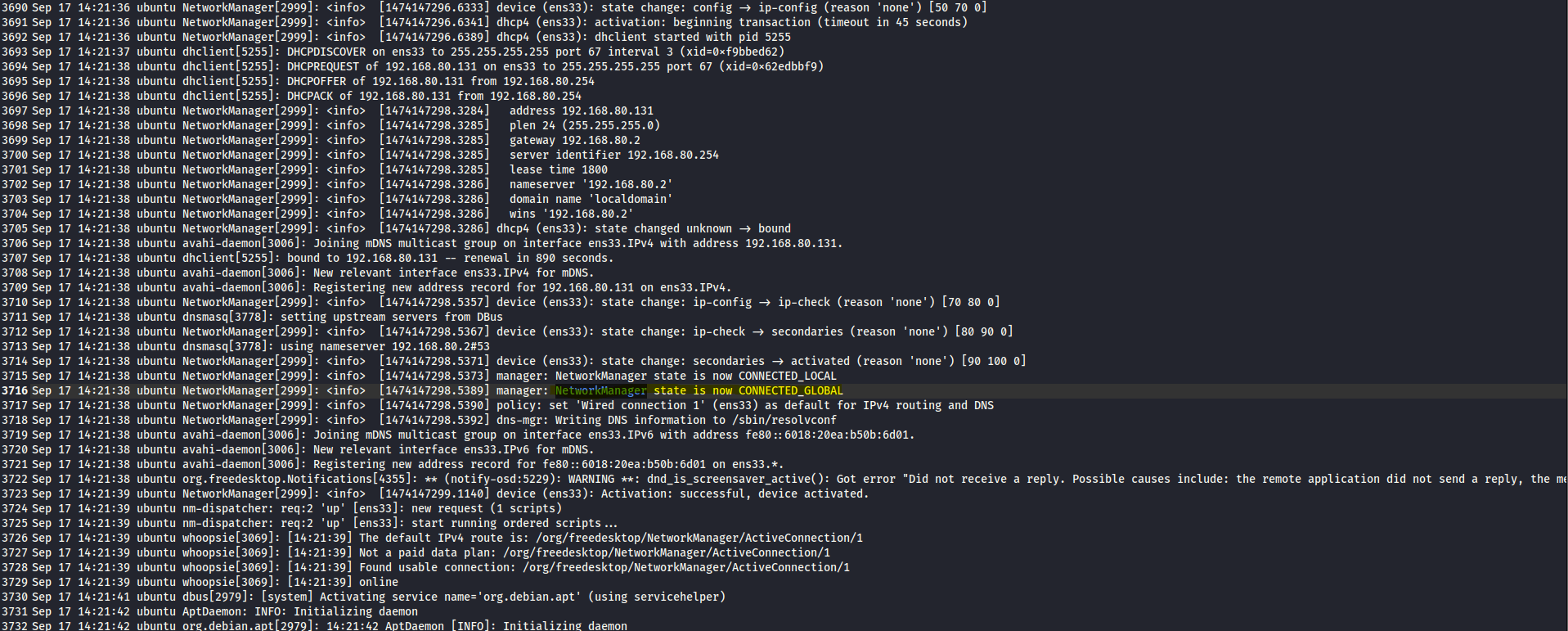
**In Syslog:**







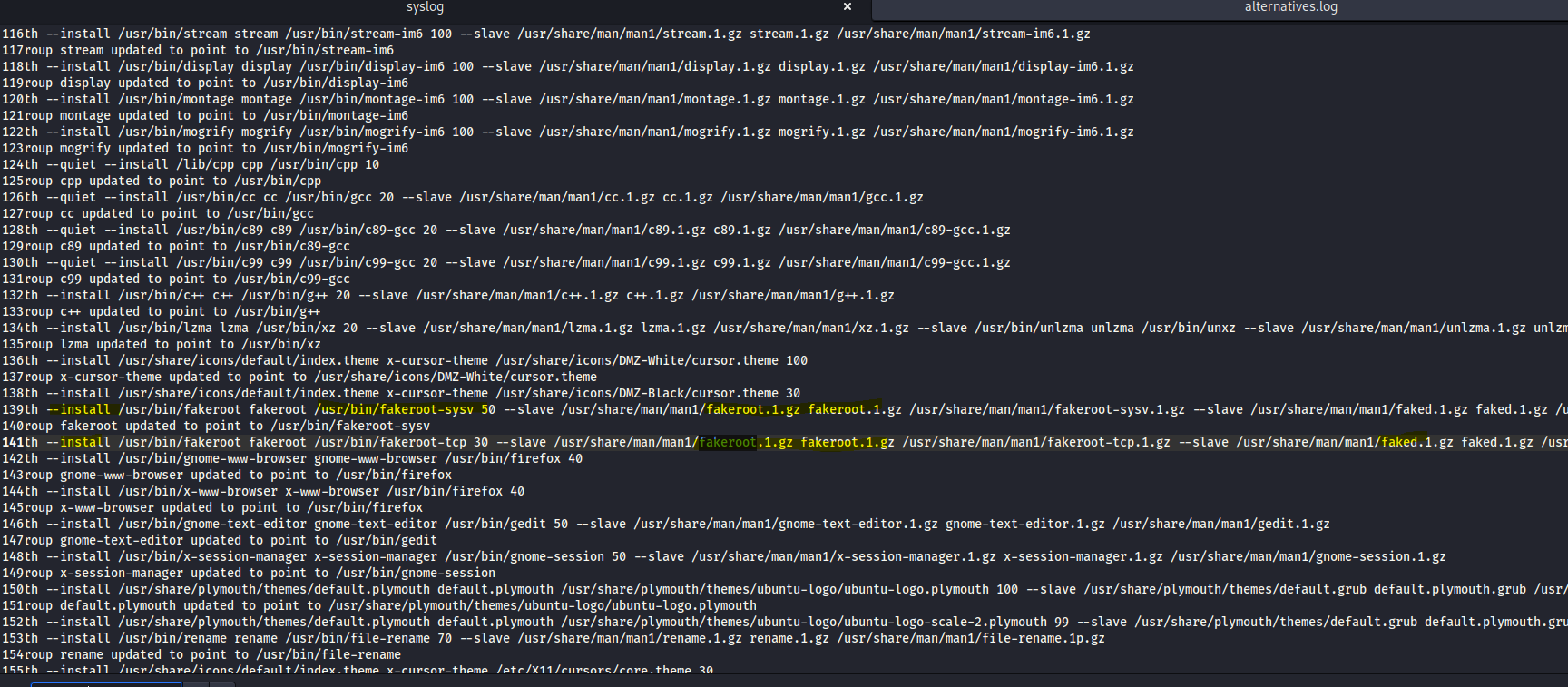
There also find out the reason for **outside staff** being accessed on the local network. And find it after analyzing the Syslog.



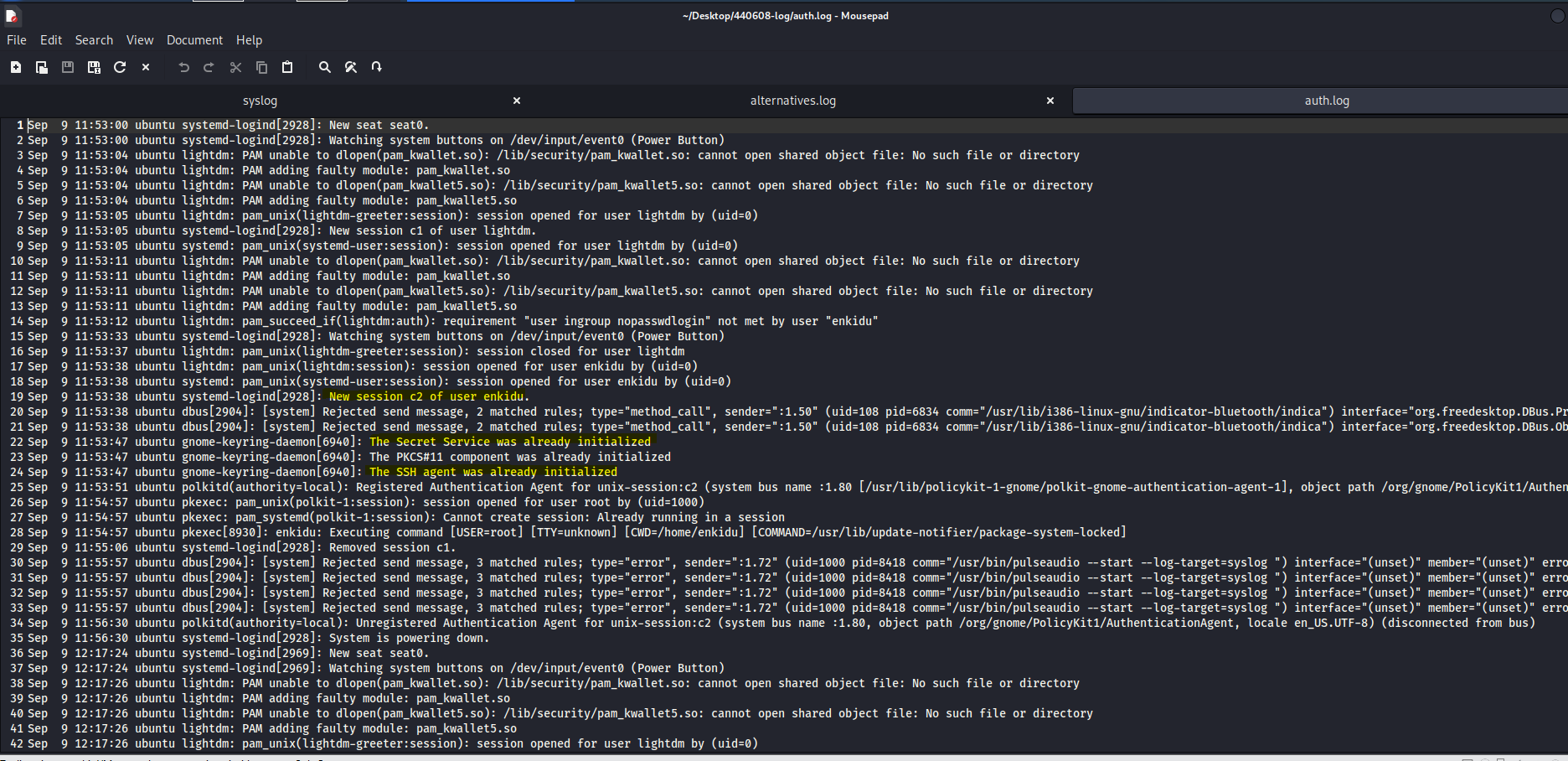
Here is the status of the network, **“NetworkManager state is now CONNECTED\_GLOBAL”**. So any staff outside can access the company’s network.

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

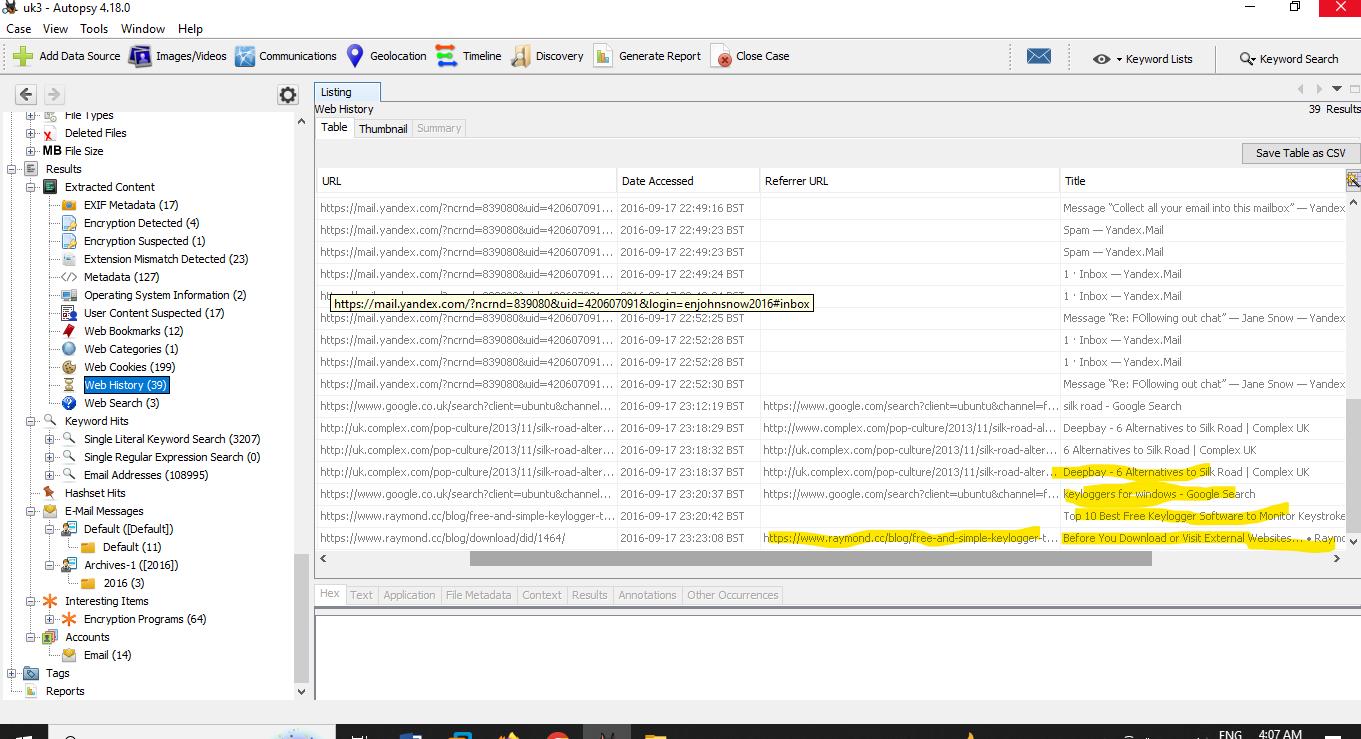
**Install fakeroot on provided VM by the local user:**

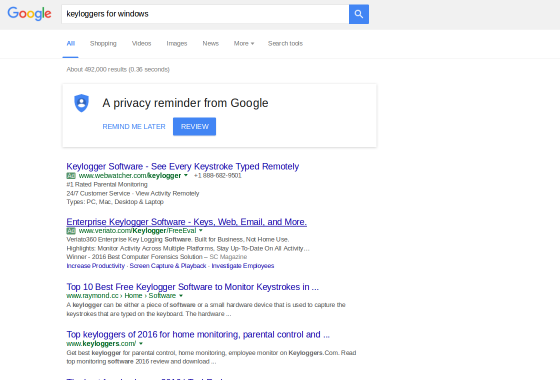
****

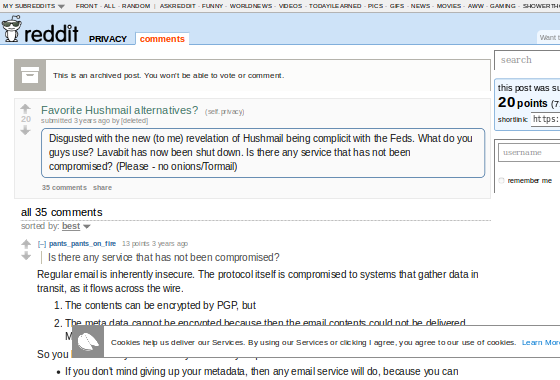
**Establish a SSH connection:**



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







# 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 |