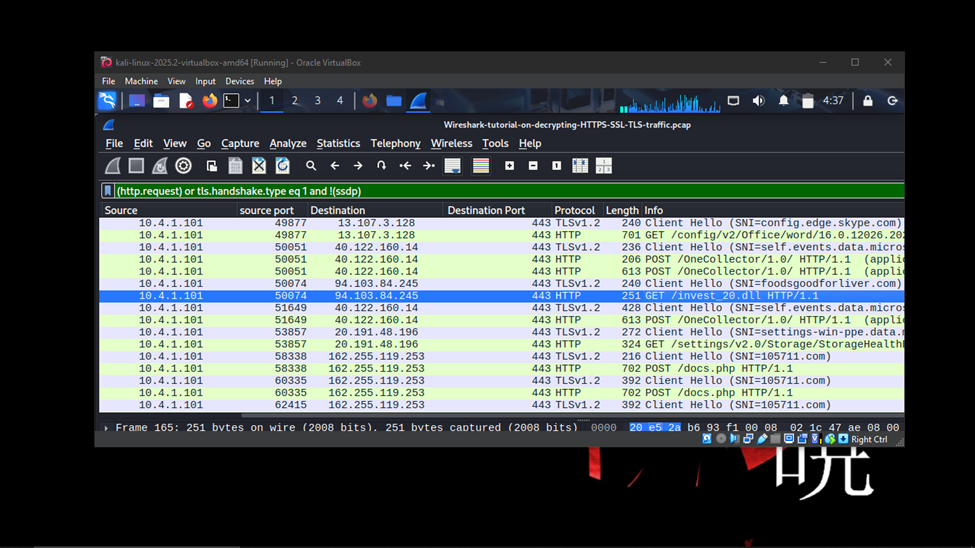
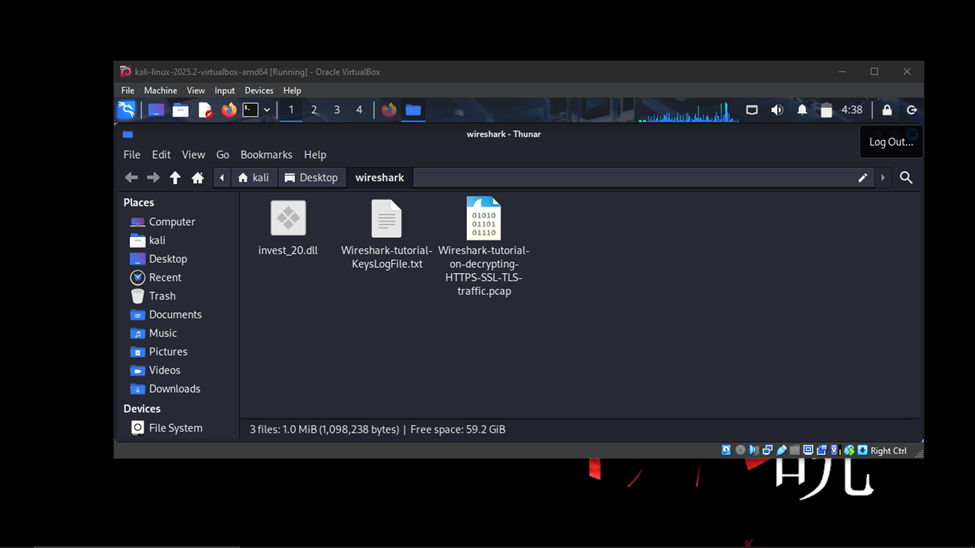
Decrypting

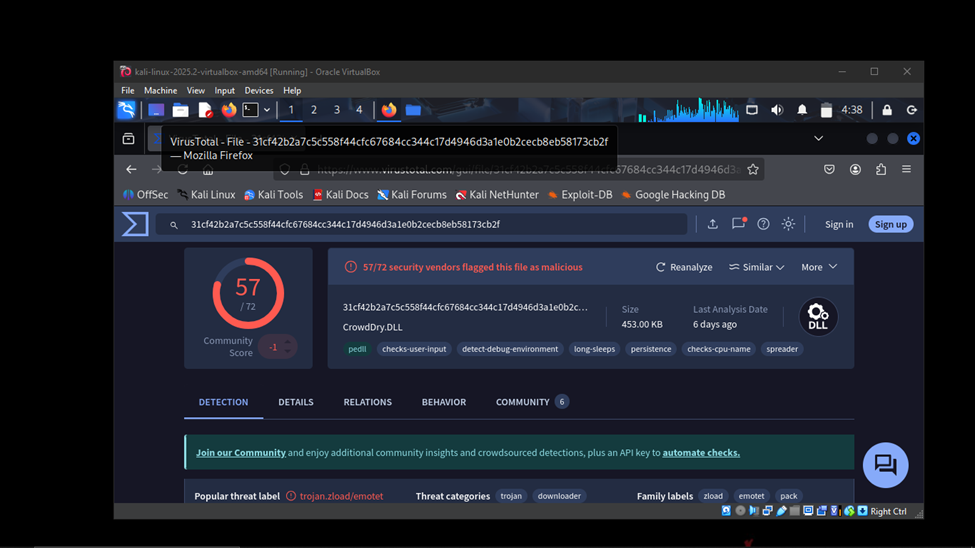
* Applied filter tls.handshake.type eq 1- for a successful handshake
* Encrypted by a ssl certificate (digital certificate that authenticates a website’s identity and enables encrypted connection between a server and browser) these are to decrypt http and ssl traffic
* Protocols – tls – premaster log file name – follow tls stream
* HTTP. Request or tls.handshake.type eq and !(ssdp), excluding ssdp reduce network noise and focuses on specific traffic



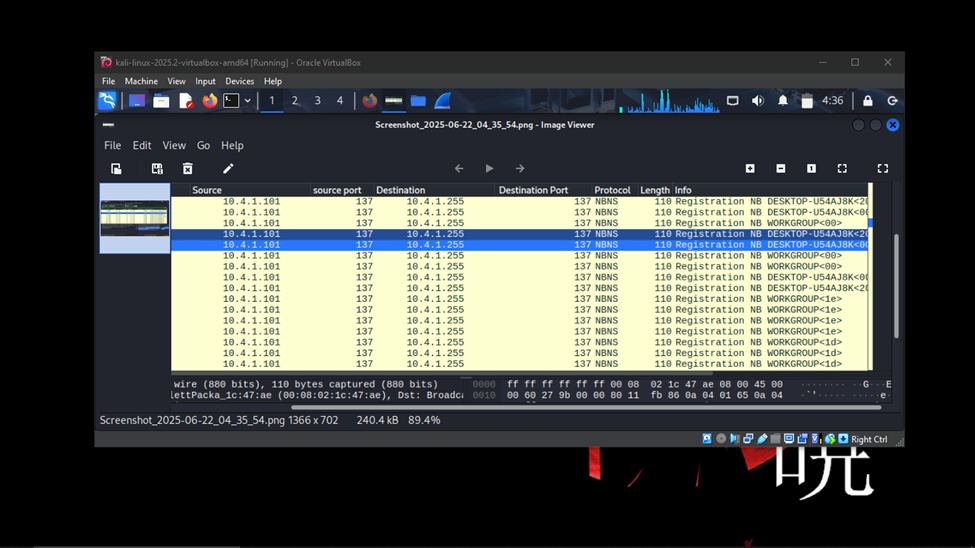
* The system infected with dridex malware, vector used was .dll
* Follow http stream of dll and download as an object
* File – export object



* Use virus total to identify type of virus



* User downloaded through email
* Post request is a method used to send data to a web server to create or update a resource, a couple were made to from … to a file called docs.php , after the infection it connects to the c2 server (these send commands to compromised devices to execute malicious actions)
* Using man in the middle proxy
* 7 0.765700 10.4.1.101 137 10.4.1.255 137 NBNS 110 Registration NB DESKTOP-U54AJ8K<00> infected system



* Command and control C2

HTTP/1.1 502 Bad Gateway

Server: mitmproxy 6.0.0.dev

Connection: close

Content-Length: 393

Content-Type: text/html

<html>

<head>

<title>502 Bad Gateway</title>

</head>

<body>

<h1>502 Bad Gateway</h1>

<p>TlsProtocolException(&#x27;Cannot establish TLS with 162.255.119.253:443 (sni: 105711.com): TlsException(&quot;SSL handshake error: SysCallError(104, \&#x27;ECONNRESET\&#x27;)&quot;)&#x27;)</p>

</body>

</html>