



Capture The Flag

NAME: MICHAEL LAMBINICIO

TEAM NAME: R3JVDXAGMQO=

Introduction

- The CTF Problem = Find Princess Leia's password.
- Steps to Solve === Start with Notepad++ & hash decrypter.
- The Solution === Decrypt the hash associated with Leia.
- Workplace Relevance = Medium to High



CTF Category Description

- Objective
 - The CTF provided a Packet Capture file to find Princess Leia's password
- Methods to solve
 - Utilizing different applications and techniques to search for certain information within the Packet Capture file
- Relation to Ethical Hacking
 - Searching within packet captured files can get you useful information about network activity and sensitive information
- Labs utilized for this problem
 - From EC-Council
 - Module 3 – Scanning Networks



Introduction to the Problem

category_06_network_captures-wireless-challenge 06-group1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.7	192.168.1.100	ICMP	74	Echo (ping) request id=0x0001, seq=51526/18121, ttl=128 (reply in 2)
2	0.000170	192.168.1.100	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=51526/18121, ttl=128 (request in 1)
3	0.748527	VMware_06:08:a5	Broadcast	ARP	42	Who has 192.168.1.100? Tell 192.168.1.8
4	0.748694	VMware_9f:f5:d6	VMware_06:08:a5	ARP	42	192.168.1.100 is at 00:0c:29:9f:f5:d6
5	0.748857	192.168.1.8	192.168.1.100	TCP	66	1268 → 110 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	0.749033	192.168.1.100	192.168.1.8	TCP	66	110 → 1268 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	0.749566	192.168.1.8	192.168.1.100	TCP	54	1268 → 110 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8	0.753800	192.168.1.8	192.168.1.100	TCP	54	[TCP ACKed unseen segment] [TCP Previous segment not captured] 1268 → 110 [FIN, ACK] Seq=52 Ack=112 Win=65536 Len=0
9	0.753946	192.168.1.100	192.168.1.8	TCP	54	[TCP ACKed unseen segment] [TCP Previous segment not captured] 110 → 1268 [ACK] Seq=112 Ack=53 Win=65536 Len=0
10	0.754022	192.168.1.100	192.168.1.8	TCP	54	110 → 1268 [FIN, ACK] Seq=112 Ack=53 Win=65536 Len=0
11	0.754111	192.168.1.8	192.168.1.100	TCP	54	[TCP ACKed unseen segment] 1268 → 110 [ACK] Seq=53 Ack=113 Win=65536 Len=0
12	1.013873	192.168.1.7	192.168.1.100	ICMP	74	Echo (ping) request id=0x0001, seq=51527/18377, ttl=128 (reply in 13)
13	1.014042	192.168.1.100	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=51527/18377, ttl=128 (request in 12)
14	2.028722	192.168.1.7	192.168.1.100	ICMP	74	Echo (ping) request id=0x0001, seq=51528/18633, ttl=128 (reply in 15)
15	2.028887	192.168.1.100	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=51528/18633, ttl=128 (request in 14)

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Ethernet II, Src: VMware_c2:a7:d8 (00:0c:29:c2:a7:d8), Dst: VMware_9f:f5:d6 (00:0c:29:9f:f5:d6)

> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.100

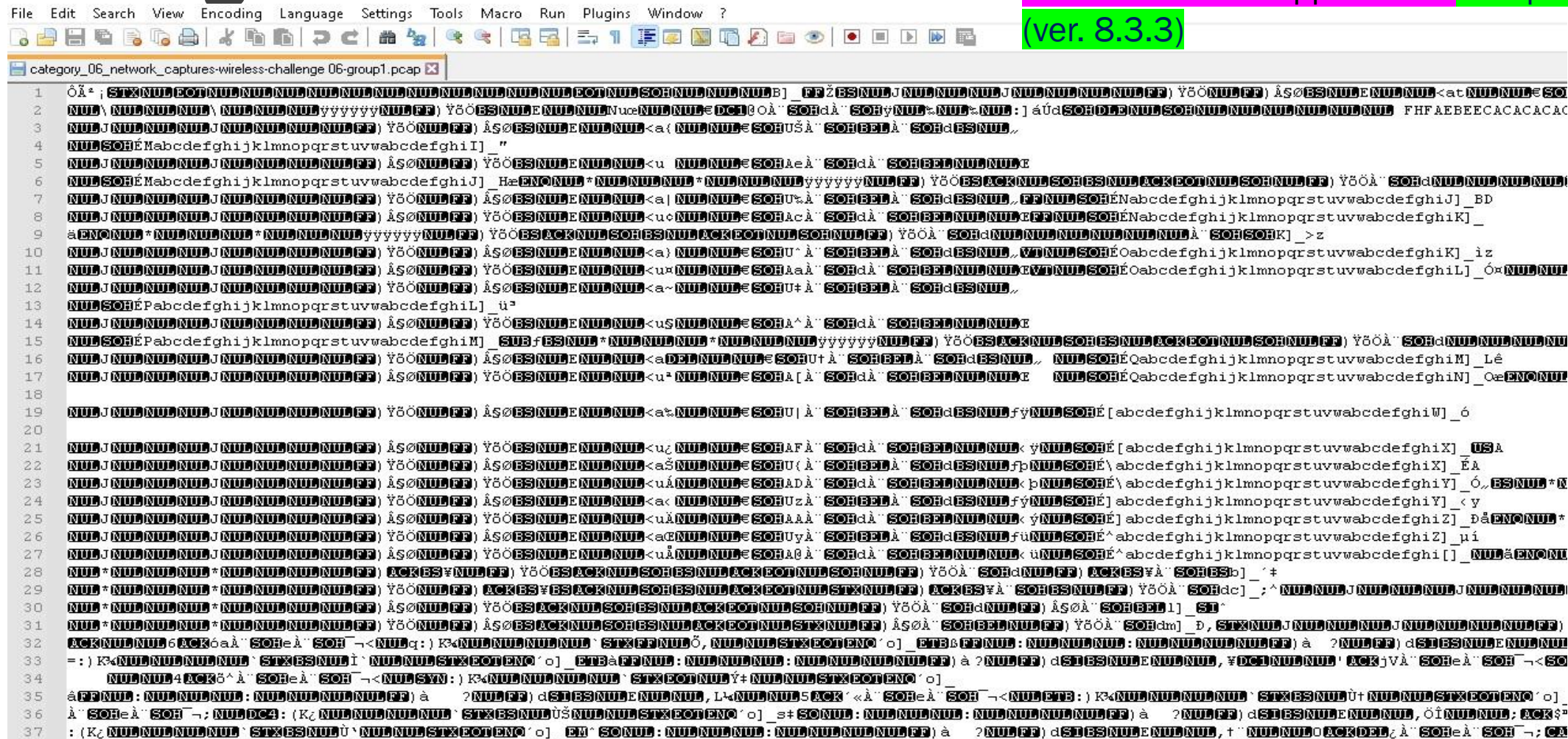
> Internet Control Message Protocol

Started with Wireshark (ver. 3.6.4) to see if I can filter out
and find the username



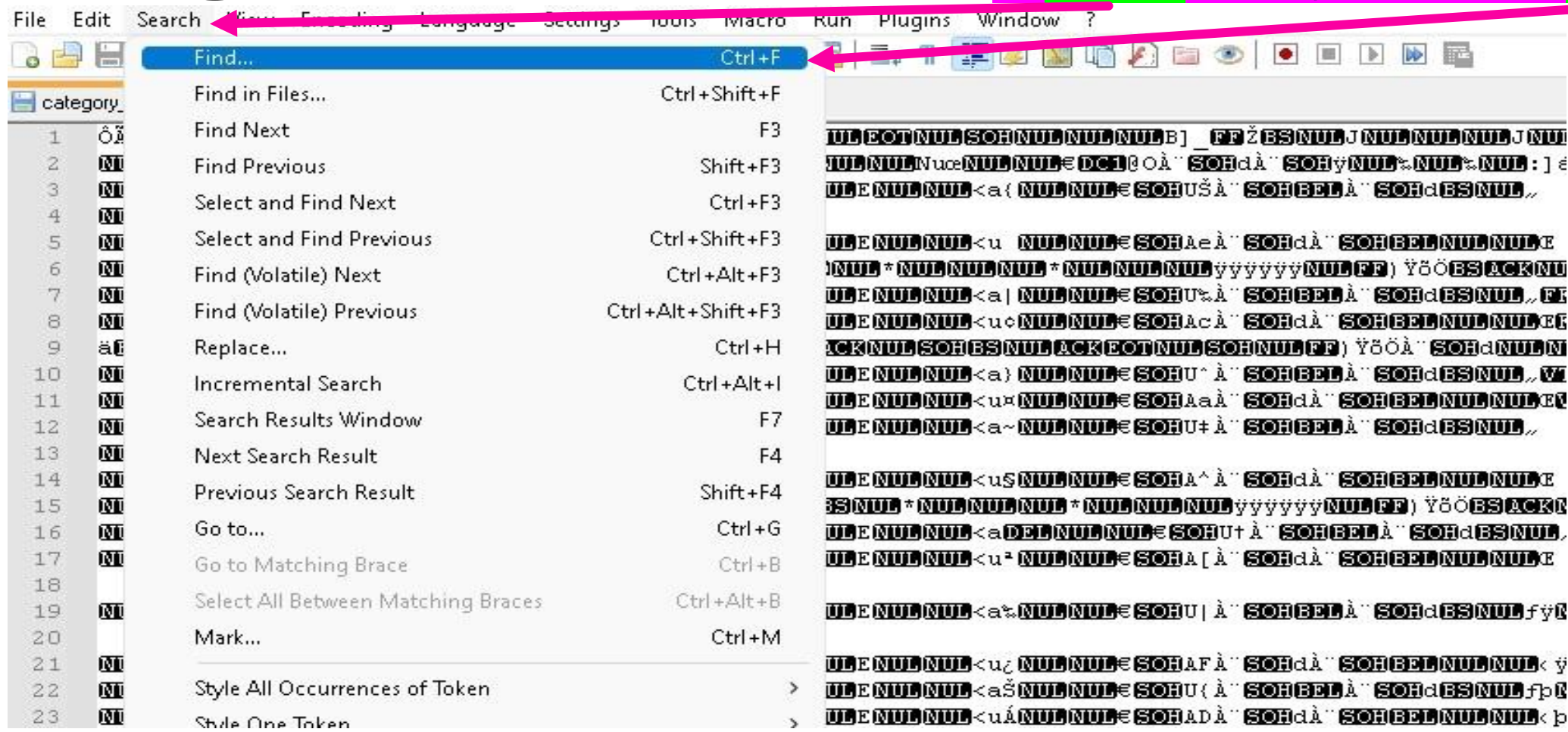
Working Toward a Solution

Unsuccessful through Wireshark, had to move to another application. Notepad++ (ver. 8.3.3)



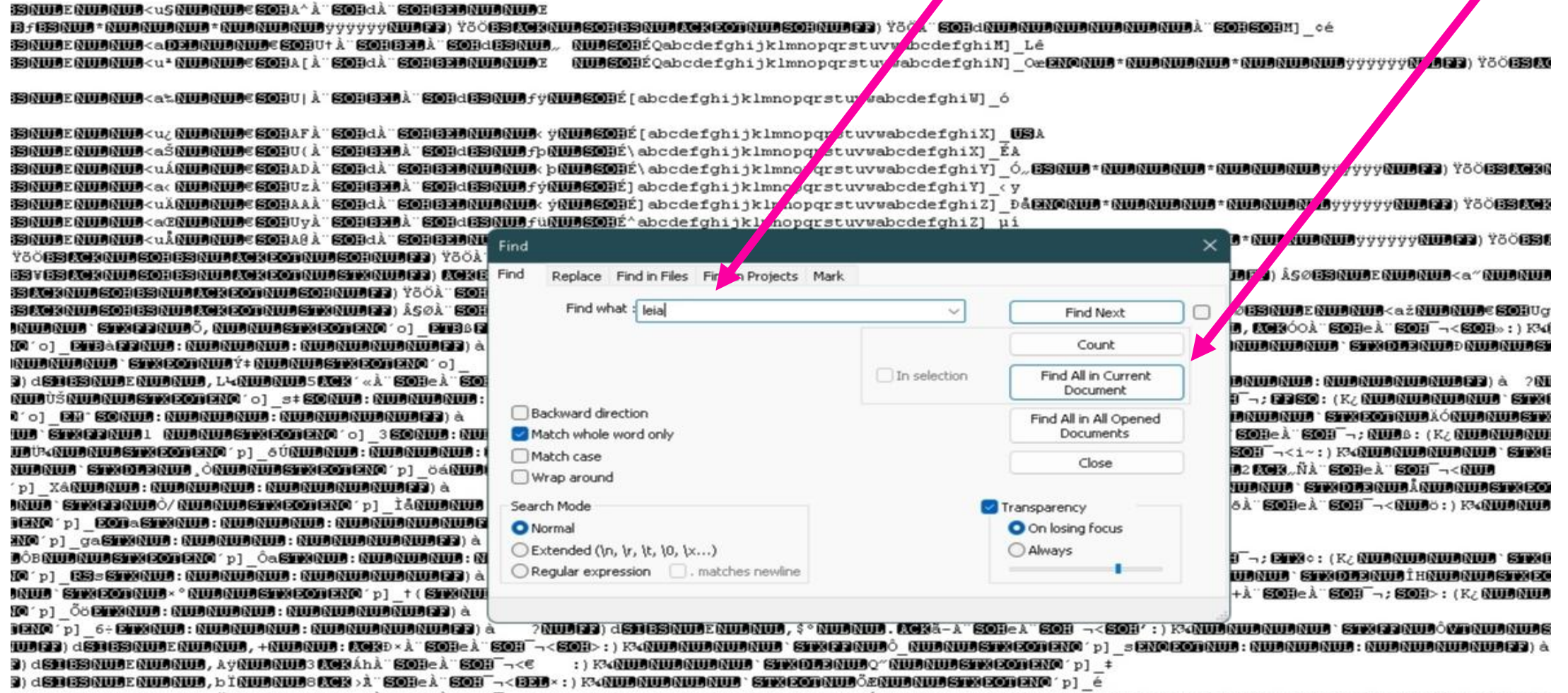
Working Toward a Solution

Hit "search" in the top tab and select "Find..."



Working Toward a Solution

Type in “leia” to search the name and click “Find All in Current Document”



Working Toward a Solution

The results are generated below...

```
4040 hacker:1004:a9a1d510b01177d1aad3b435b51404ee:afc44ee7351d61d00698796d506b1ebf:::
4041 HelpAssistant:1000:56991ec2debe0a22379753c3550506a8:535b8a5cb471c874715fa13259623614:::
4042 IUSR_WINXP:1017:b38a8793d0549054c29621c527673248:34fb426f13af9aad4a3a85381c11631c:::
4043 leia:1012:088870ba8ea71662aad3b435b51404ee:4619c592fda516c8140495d2fbf707fc:::
4044 luke:1011:6a47580eb4df42a5aad3b435b51404ee:e9776ecb486cc1d7780310de53b30588:::
4045 r2d2:1014:dc2031e004699438aad3b435b51404ee:affe9616fbd19e3a14447309962e477:::
4046 stormtrooper:1015:dca7d3c500543d6baad3b435b51404ee:c705690627d5de4c57e4e78e01a14eaa:::
4047 SUPPORT_388945a0ENQnetCachSTX:1002:aad3b435b51404eeaaad3b435b51404ee:9765e54143f42ee07ec69cee5b4280c3:::
4048 vader:1010:7b96b77a223162b1aad3b435b51404ee:2c8a51b3b72395d6f3623a0b7c4f1cfa:::
4049 victim:1005:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
4050 yoda:1016:828a670f0fd85ea7aad3b435b51404ee:cf7c4e71bd9d719e05aa399c6f528b5:::
4051 NULNULNULNULFFNULSTXNULPOTNULNULNULNULÓ`_h`VTNUL6NULNULNUL6NULNULNULNULFF)à?NULFF)dSTIBSNULENULNUL(Ûy@NUL@ACKÜRÀ`SOH
4052 ...PDELEGS`"QNULNULÔ`_RSgETXNULJNULNULNULJNULNULNULNULFF)YöÖNULFF)ÎSøBSNULENULNUL<e*NULNULeSOHQÜÀ`SOHBELÀ`SOHdBSNULeNUL
4053 NUL*NULNULNUL*NULNULNULNULFF)ÎSøNULFF)YöÖBSACKNULSOHESNULACKREOTNULSOHNULFF)YöÖÀ`SOHdNULFF)ÎSøÀ`SOHBELÚ`_H+
4054 NUL*NULNULNUL*NULNULNULNULFF)YöÖNULFF)ÎSøBSACKNULSOHESNULACKREOTNULSTXNULFF)ÎSøÀ`SOHBELNULFF)YöÖÀ`SOHdÚ`_?dSTXNULxNUL
4055 HOST: 239.255.255.250:1900
4056 MAN: "ssdp:discover"
4057 MX: 1
4058 ST: urn:dial-multiscreen-org:service:dial:1
4059 USER-AGENT: Google Chrome/86.0.4240.75 Windows
```

Search results - (1 hit)

Search "leia" (1 hit in 1 file of 1 searched)

C:\Users\Hidden Gem\Desktop\CMIT321\Project 2\category_06_network_captures-wireless-challenge 06-group1.pcap (1 hit)

Line 4043: leia:1012:088870ba8ea71662aad3b435b51404ee:4619c592fda516c8140495d2fbf707fc:::

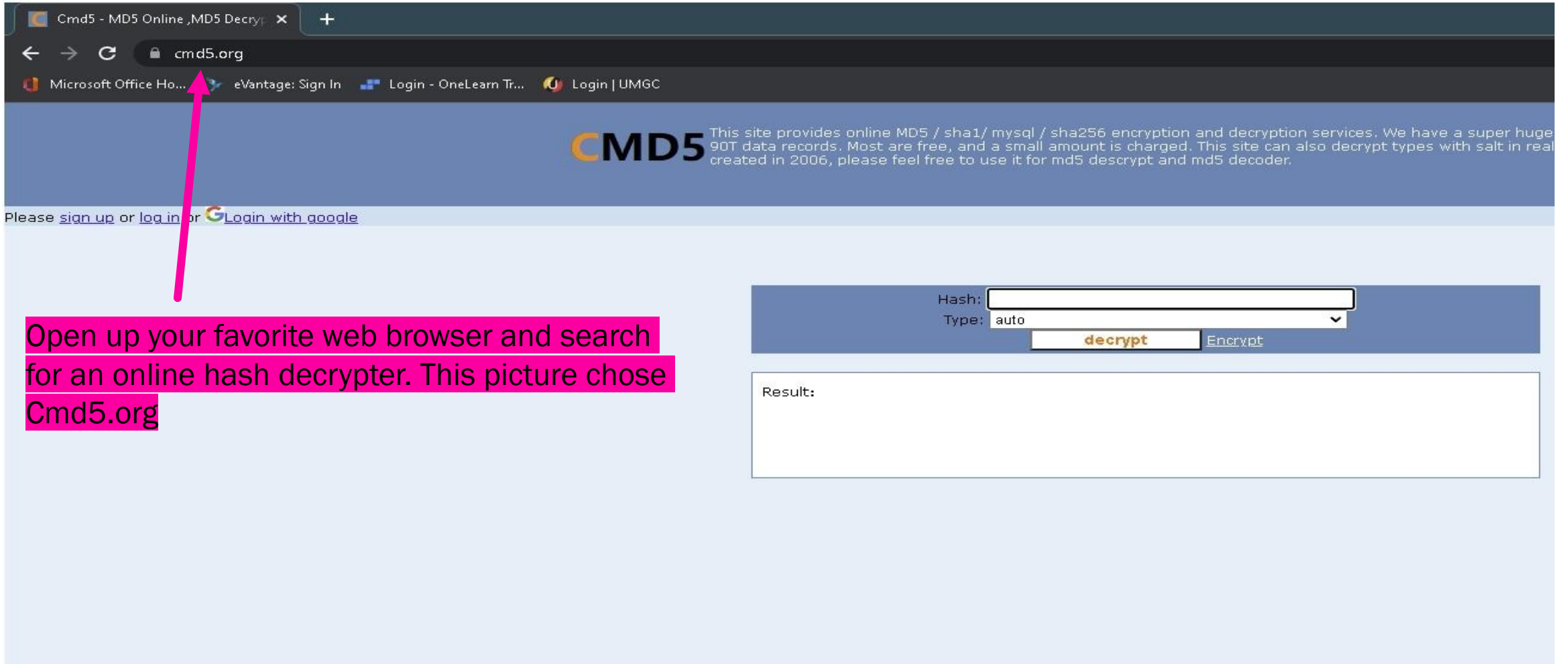
Search "leia" (1 hit in 1 file of 1 searched)

Copy the hash on the far right to decrypt

Normal text file



Working Toward a Solution



The screenshot shows a web browser window with the address bar displaying "cmd5.org". The browser's tab bar shows "Cmd5 - MD5 Online ,MD5 Decryp". The website header features the "CMD5" logo and a description: "This site provides online MD5 / sha1/ mysql / sha256 encryption and decryption services. We have a super huge 90T data records. Most are free, and a small amount is charged. This site can also decrypt types with salt in real created in 2006, please feel free to use it for md5 decrypt and md5 decoder." Below the header, there are links for "sign up", "log in", and "Login with google". The main content area has a form with a "Hash:" input field, a "Type:" dropdown menu set to "auto", and two buttons: "decrypt" and "Encrypt". Below the form is a "Result:" label and a large empty text box for the output.

Open up your favorite web browser and search for an online hash decrypter. This picture chose Cmd5.org



Arriving at the Solution

- After finding the hash, simply copy and paste it in the Hash text box and hit decrypt to retrieve the password.

Tr... Login | UMG

CMD5 This site provides online MD5 / sha1/ mysql / sha256 encryption and decryption services. We have a super huge database with more than 90T data records. Most are free, and a small amount is charged. This site can also decrypt types with salt in real time. This site was created in 2006, please feel free to use it for md5 decrypt and md5 decoder.

Copied hash → Hash: 4619c592fda516c8140495d2fb707fc

Type: NTLM

decrypt Encrypt

Result:
sister

Decrypted, revealing Leia's password



Strategies, Pitfalls, Lessons Learned

- Strategies

- Using Wireshark to search for the username on the packet capture file did not work. Learned to search within a different application (Notepad++) to obtain the username. Understanding that the password was a hash, used an online decrypter to decrypt and obtain the password.

- Pitfalls

- Relying on a single application to find the answer.

- Lessons Learned

- Your first choice of application may not always work in finding the answer you are looking for. Learning other applications can be useful to jump start your search criteria. Also utilizing online sources to help provide the solutions.



The Relationship to the Workplace

- Using alternative methods in finding a solution is highly recommended as sometimes, having only one method could also be a single point of failure. Having different tactics can expose weaknesses within their system. But it can also help you strategize on how to prevent it.



Summary

- Sometimes, relying on just one application may not get you the answer you need, even if using technical application such as Wireshark. There are various tools that are simple as notepad that can make searching for usernames easy. When you understand coding and hashes, you then can utilize resources online to complete your problem.
- Most username/passwords aren't show in plain site and sometimes going through different steps with alternate tools are necessary to find them. This shows that your username/password are never truly protected, but why most organizations manage the account policies by having workers change their passwords frequently.



References

- “What is notepad++,” *Notepad++*. [Online]. Available: <https://notepad-plus-plus.org/>. [Accessed: 26-Apr-2022].
- “Wireshark,” *Wireshark · Go Deep*. [Online]. Available: <https://www.wireshark.org/#learnWS>. [Accessed: 26-Apr-2022].
- “MD5 online ,MD5 decryption, MD5 Hash Decoder,” *Cmd5*. [Online]. Available: <http://www.cmd5.org/>. [Accessed: 26-Apr-2022].