ANALÝZA VZŤAHOV MEDZI FORENZNÝMI ARTEFAKTAMI S VYUŽITÍM TEÓRIE GRAFOV

Vedúci práce: doc. RNDr. JUDr. Pavol Sokol, PhD.
Konzultant: RNDr. Eva Marková

Sophia Petra Krišáková

MOTIVÁCIA

- nárast počtu útokov
- výskyt incidentu a jeho identifikácia

  100 – 200 dní
- reakčný čas

  50 – 70 dní
- zníženie tohto času
- vyhľadávanie vzťahov medzi forenznými artefaktami pomocou grafov
- rýchlejšia reakcia na bezpečnostný incident

THE CASE OF THE STOLEN SZECHUAN SAUCE

- DFIR MADNESS
- Disk image
- Vytvorenie časovej osi – log2timeline
- Výstup vo formáte plaso – l2tcsv
- Supertimeline: Date, Time, Timezone, MACB, Source, Sourcetype, Type, User, Host, Short, Desc, Version, Filename, Inode, Notes, Format, Extra
- 11 rôznych rámcov - FILE, EVT

Zdroj obrázka: https://dfirmadness.com/the-stolen-szechuan-sauce/

https://dfirmadness.com/the-stolen-szechuan-sauce/

SÚBORY A INODY RELEVANTNÉ PRE PRÍPAD

- File inodes: 84630, 84880, 84987, 86966, 86967, 86968, 86970, 86971, 86975, 87059, 87060, 87064, 87111, 87112, 87137;
- File names: "coreupdater.exe", "FILESH 1", "Secret", "BETH_S 1.TXT", "Beth_Secret.lnk", "SECRET 1.TXT", "SECRET_beth.lnk", "Szechuan", "SZECHU 1.TXT", "Secret.lnk", "NoJerry.lnk", "No-Jerry.txt", "f01b4d95cf55d32a.automaticDestinationsms", "SECRET_beth.txt", "Beth_Secret.txt", "Secret.zip", "coreupdater.exe.2424urv.partial"

GRAFY

- reprezentácia vzťahov medzi dátami – vrcholy a hrany
- grafické zobrazenie
- prehľadnosť
- excentricita vrcholov
- bipartitnosť
- súvislosť
- stromy, cesty, cykly

ĎALŠIE DATASETY

- Magnet CTF
  - 2019
  - 2020
  - 2022
- Data Leakage Case
  - NIST Hacking Case
  - NIST Data Leakage Case

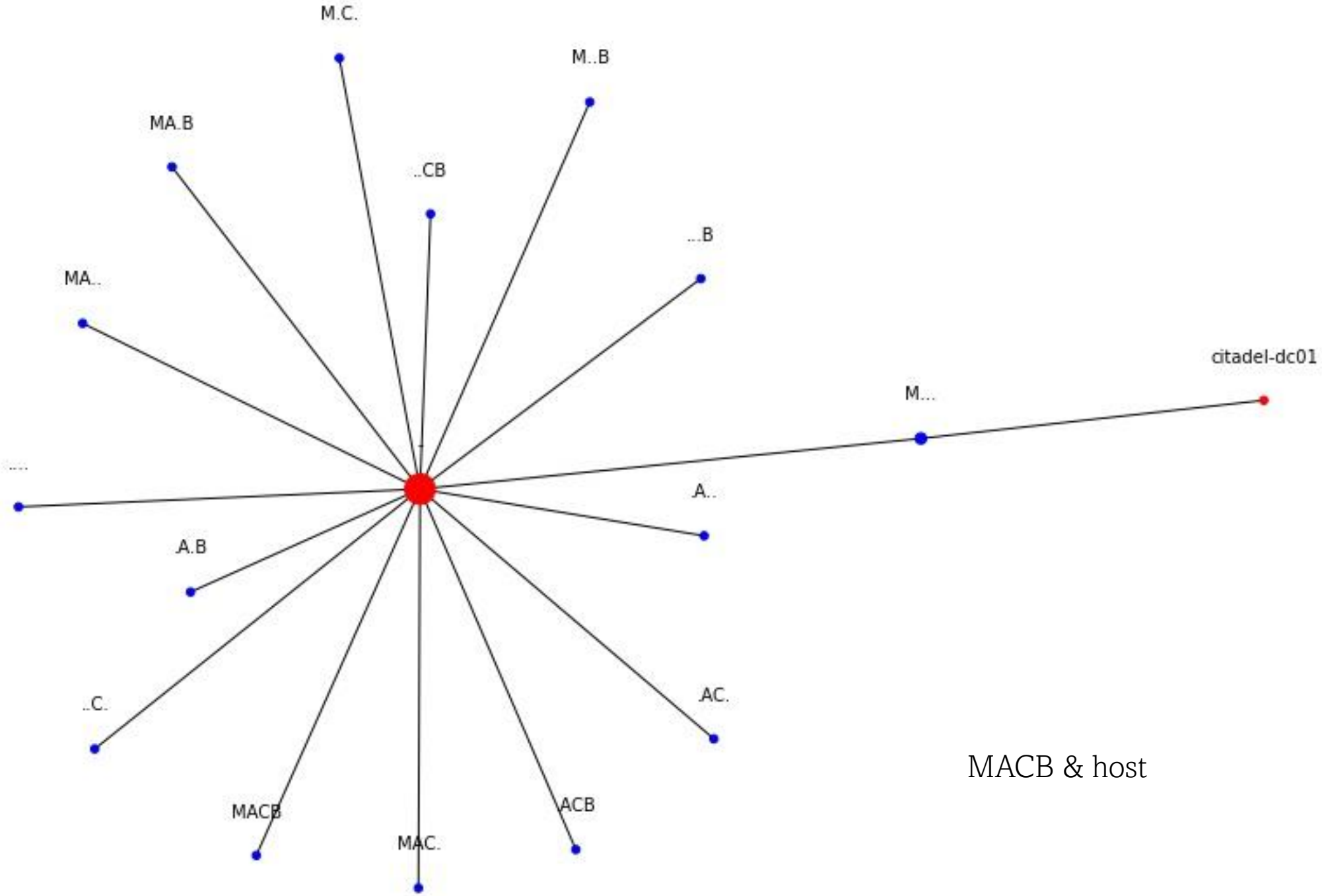
https://digitalcorpora.s3.amazonaws.com/corpora/scenarios/magnet/2019%20CTF%20-%20Windows-Desktop.zip
https://digitalcorpora.s3.amazonaws.com/corpora/scenarios/magnet/2020%20CTF%20-%20Windows.zip
https://digitalcorpora.s3.amazonaws.com/corpora/scenarios/magnet/2022%20CTF%20-%20Windows.zip
https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html

PROCES VYTVÁRANIA GRAFU

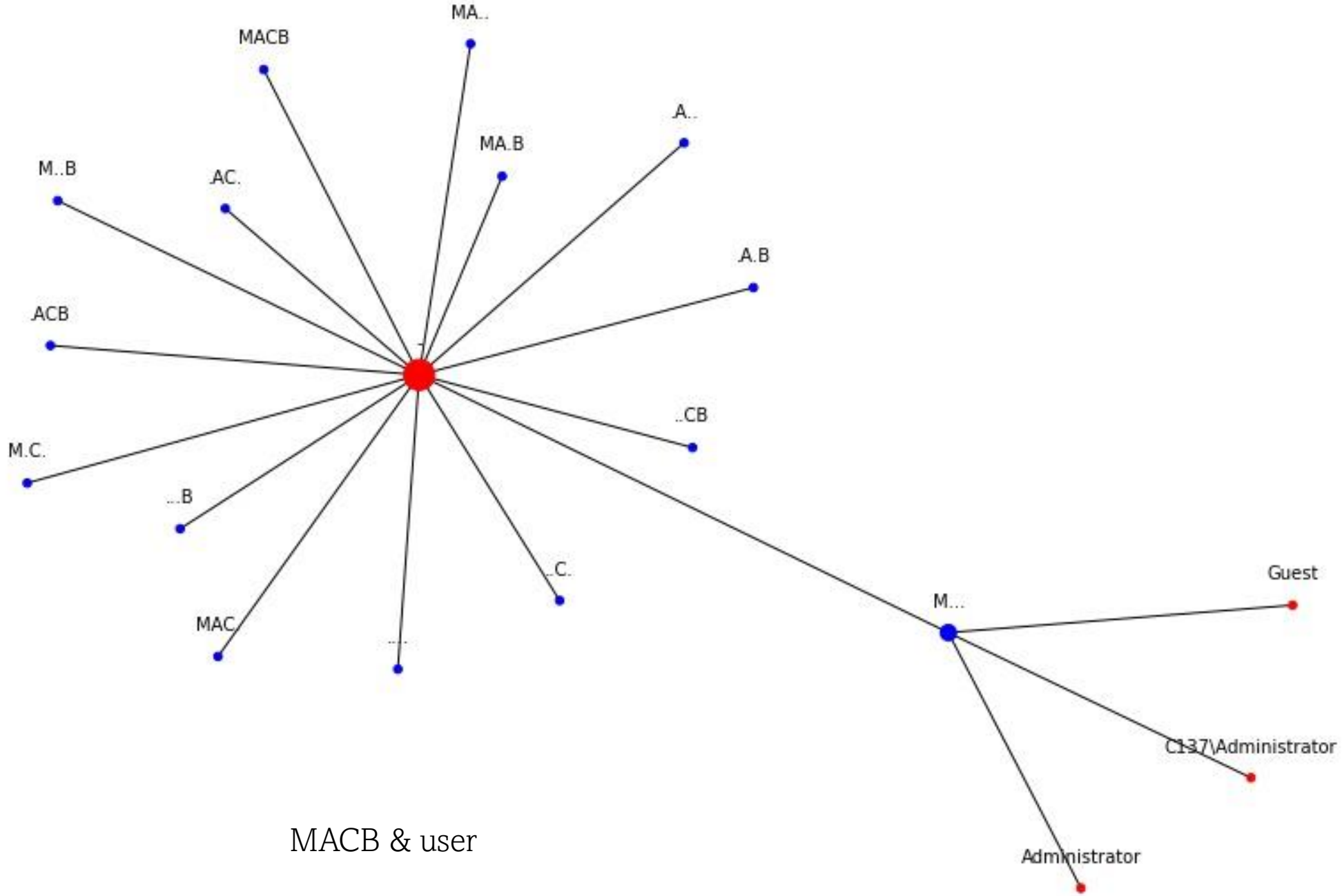
```
date (268,)
time (20682,)
timezone (2,)
MACB (15,)
source (11,)
sourcetype (34,)
type (27,)
user (4,)
host (2,)
short (373451,)
desc (826489,)
version (1,)
filename (111972,)
inode (98116,)
notes (1,)
format (45,)
extra (235896,)
```

```
1 df[["MACB","source","sourcetype", "type","user","host", "inode", "format"]]
```

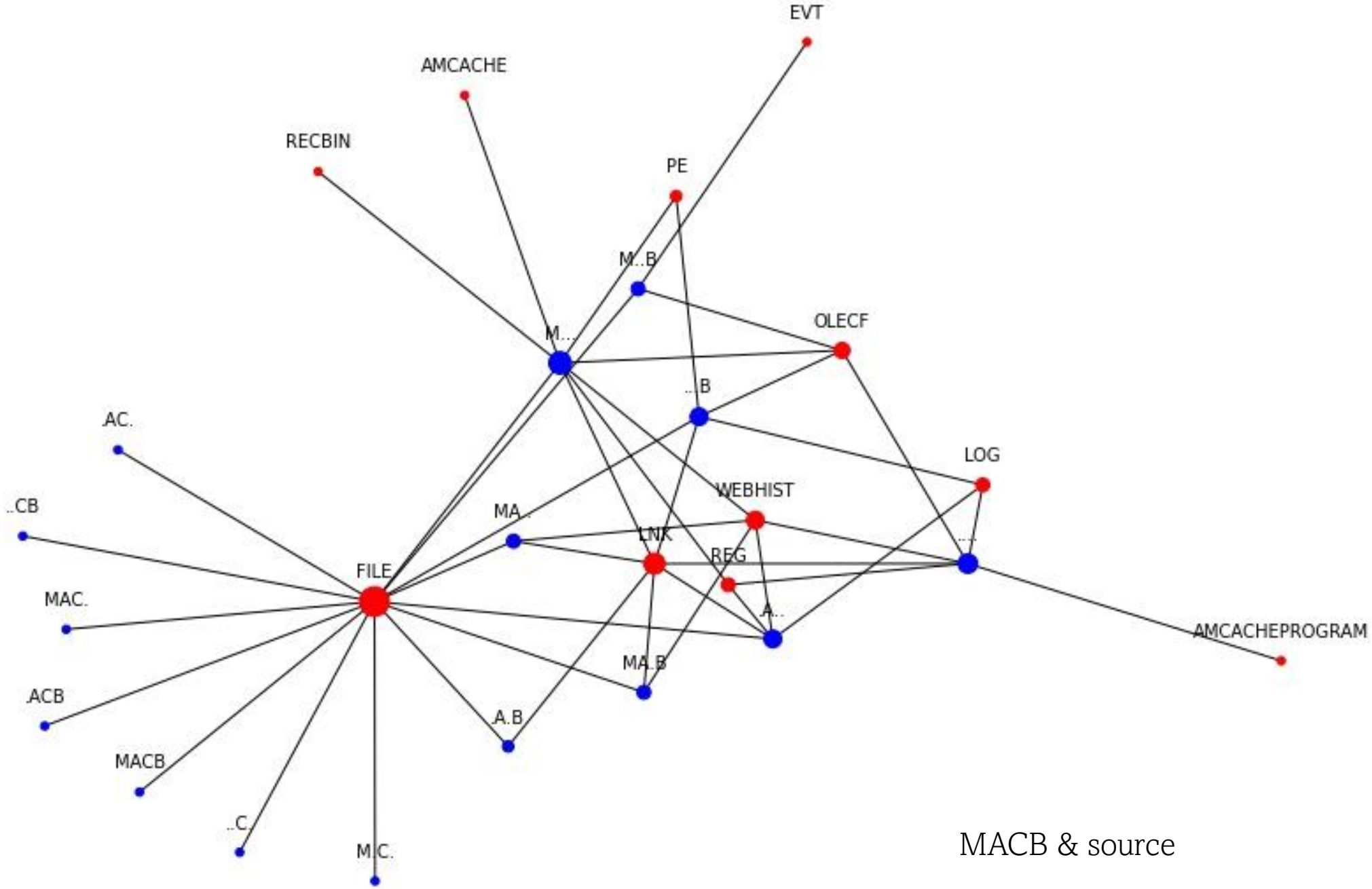
	MACB	source	sourcetype	type	user	host	inode	format
0	....	LOG	System	Installation Time	-	-	78036	winreg/windows_version
1	.A..	REG	Registry Key - UserAssist	Last Time Executed	-	-	84874	winreg/userassist
2	.A..	REG	Registry Key - UserAssist	Last Time Executed	-	-	84874	winreg/userassist
3	.A..	REG	Registry Key - UserAssist	Last Time Executed	-	-	84874	winreg/userassist
4	.A..	REG	Registry Key - UserAssist	Last Time Executed	-	-	84874	winreg/userassist
...	...	...	...	...	...	...	...	...
1263782	M...	PE	PE Import Time	Content Modification Time	-	-	37022	pe
1263783	M...	PE	PE Import Time	Content Modification Time	-	-	34311	pe
1263784	M...	PE	PE Import Time	Content Modification Time	-	-	34311	pe
1263785	M...	PE	PE Import Time	Content Modification Time	-	-	37022	pe
1263786	M...	PE	PE Import Time	Content Modification Time	-	-	37022	pe



MACB & host


MA..
MACB
A..
MA.B
M..B
.AC.
A.B
.ACB
..CB
M.C.
...B
..C.
MAC.
....
M...
Guest
C137\Administrator
Administrator

MACB & user


EVT
AMCACHE
RECBIN
PE
M..B
OLECF
M...
..B
AC.
LOG
WEBHIST
..CB
MA..
LNK
REG
....
FILE
MAC.
A...
AMCACHEPROGRAM
MA.B
.ACB
A.B
MACB
..C
M.C.

MACB & source


Content Modification Time; Last Access Time
Content Modification Time; Creation Time; Last Access Time
MACB
MA.B Content Modification Time; Creation Time; Last Access Time; Metadata Modification Time
Creation Time; Last Access Time; Metadata Modification Time
ACB
Start Time
Last Shutdown Time
Last Time Executed
Last Connection Time
Content Modification Time; Creation Time
Creation Time; Last Access Time
Content Deletion Time
Content Modification Time
Last Access Time; Metadata Modificati
Content Modification Time; Metadata Modification Time
M.C.
Synchronization time
Installation time
last registered time
Document Last Creation Time
Content Modification Time; Last Access Time; Metadata Modification Time
MAC.
Creation Time
Metadata Modification Time

MACB & type

- zúženie datasetu na dáta s časovou pečiatkou ‘M…’
- z pôvodných 1 263 787 riadkov v datasete -> 397 060
- filtrácia, podľa: ‘host’ = ‘citadel-dc01’ – 6 záznamov
  - inode: 86968, 86970
  - filename: 9b9cdc69c1c24e2b.automaticDestinations-ms, f01b4d95cf55d32a.automaticDestinations-ms
  - time: 03:31:50 – 03:35:07
  - date: 19.09.2020
- filtrácia, podľa: ‘type’ = 'Content Deletion Time‘ – 1 záznam
  - source: RECBIN
  - short: Deleted file: C:\FileShare\Secret\SECRET_beth.txt
  - time: 03:34:27
  - date: 19.09.2020

```
1 dx[dx["user"]== 'Guest']
```

	date	time	timezone	MACB	source	sourcetype	type	user	host	short	desc	ve
1160001	09/17/2020	17:57:10	UTC	M...	REG	Registry Key - User Account Information	Content Modification Time	Guest	-	Guest RID: 501 Login count: 0	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Us...	

```
1 dx[dx["user"]== 'C137\Administrator']
```

	date	time	timezone	MACB	source	sourcetype	type	user	host	short	
1258989	09/19/2020	03:36:25	UTC	M...	REG	Registry Key - RDP Connection	Content Modification Time	C137\Administrator	-	[HKEY_CURRENT_USER\Software\Microsoft\Terminal...	[H

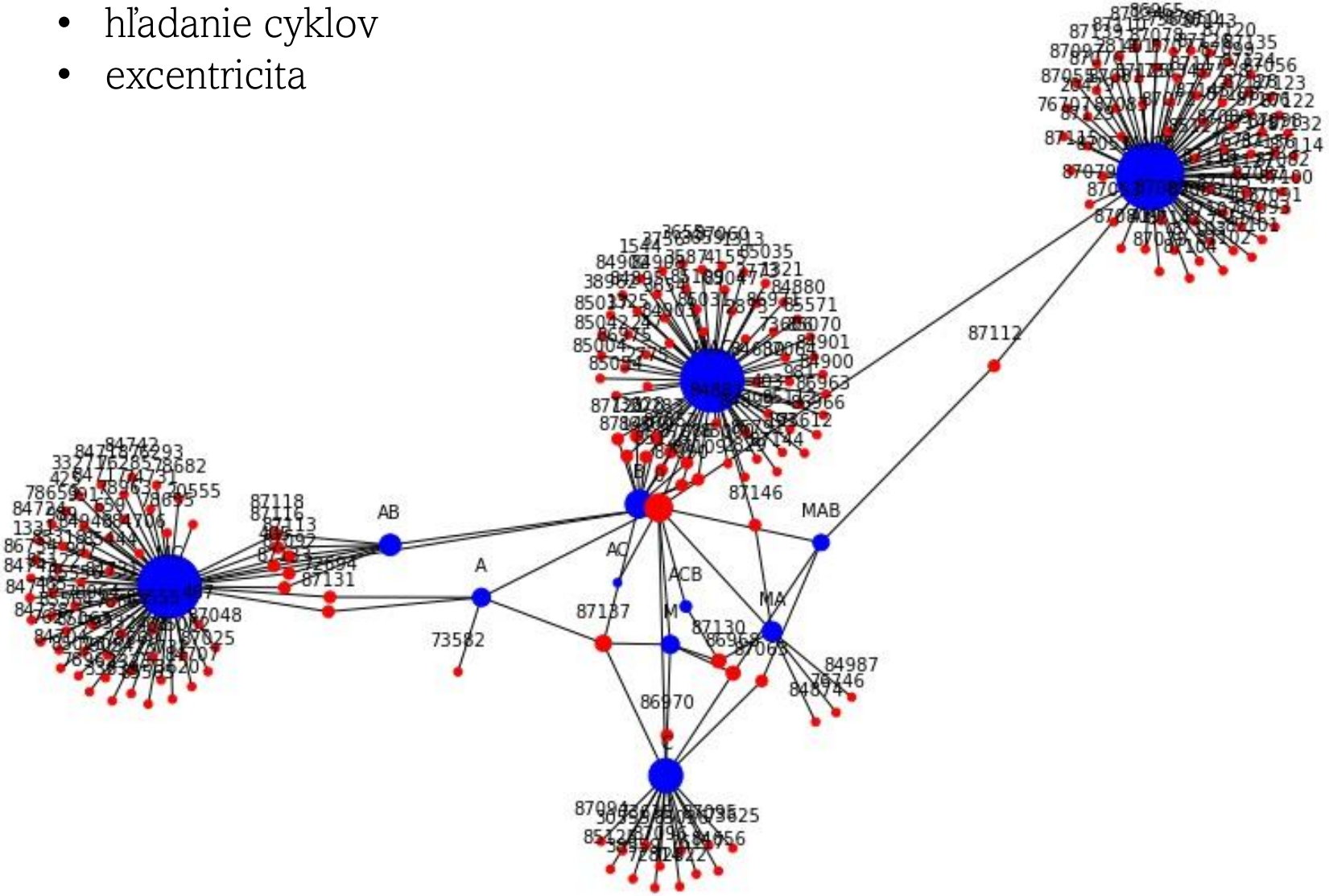
```
1 dx[dx["user"]== 'Administrator']
```

	date	time	timezone	MACB	source	sourcetype	type	user	host	short	
1160000	09/17/2020	17:57:10	UTC	M...	REG	Registry Key - User Account Information	Content Modification Time	Administrator	-	Administrator RID: 500 Login count: 0	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Acc

D C - F I L E

- 40 stĺpcov
- MACB – ‘M’, ‘A’, ‘C’, ‘B’
- Výsledky zo supertimeline – 19.09.2020 – iba tento deň

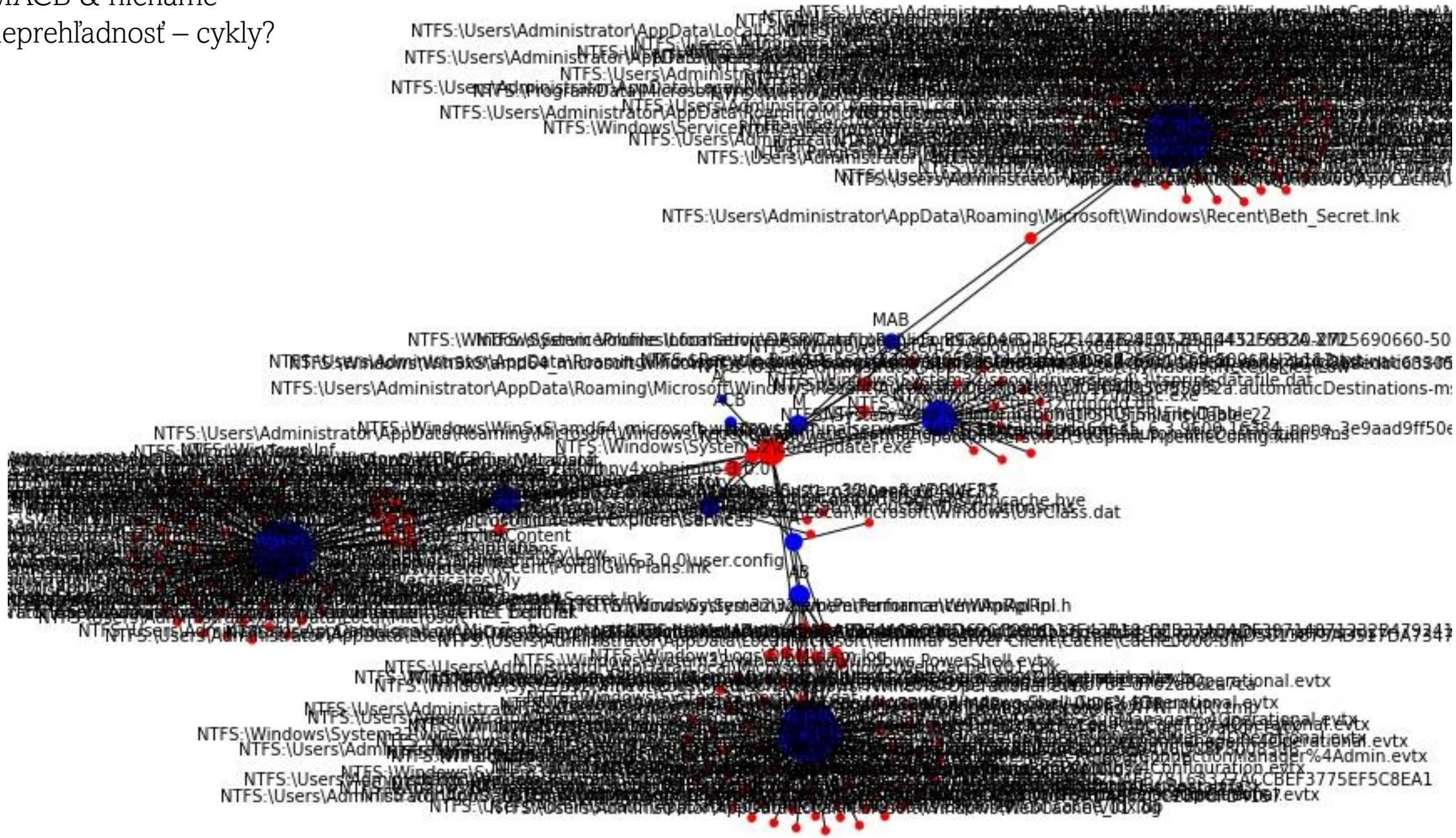
- graf nie je strom
- hľadanie cyklov
- excentricita



MACB & inode

```
Cyklus: ['C', 87063, 'MAB', 0]
Cyklus: ['MACB', 87112, 'MAB', 0]
Cyklus: ['M', 86968, 'MAB', 0]
Cyklus: ['C', 86968, 'MAB', 0]
Cyklus: ['MAC', 87146, 'MA', 0]
Cyklus: ['M', 87130, 'MA', 0]
Cyklus: ['ACB', 87130, 'MA', 0]
Cyklus: ['MC', 72694, 'A', 0]
Cyklus: ['MC', 87131, 'A', 0]
Cyklus: ['M', 87137, 'A', 0]
Cyklus: ['B', 87137, 'A', 0]
Cyklus: ['C', 87137, 'A', 0]
Cyklus: ['C', 86970, 'M', 0]
Cyklus: ['MC', 405, 'AB', 0]
Cyklus: ['MC', 87133, 'AB', 0]
Cyklus: ['MC', 87113, 'AB', 0]
Cyklus: ['MC', 87092, 'AB', 0]
Cyklus: ['MC', 87118, 'AB', 0]
Cyklus: ['MC', 87116, 'AB', 0]
Cyklus: ['MAC', 73628, 'B', 0]
Cyklus: ['MAC', 87121, 'B', 0]
Cyklus: ['MAC', 87052, 'B', 0]
Cyklus: ['MAC', 87140, 'B', 0]
Cyklus: ['MAC', 87109, 'B', 0]
Cyklus: ['MAC', 87090, 'B', 0]
Cyklus: ['MAC', 87086, 'B', 0]
Cyklus: ['MAC', 86800, 'B', 0]
Cyklus: ['MAC', 85126, 'B', 0]
Cyklus: ['MAC', 20283, 'B', 0]
```

- MACB & filename
- neprehľadnosť – cykly?



```
Cyklus: ['NTFS:\\$MFT', 'C', 'NTFS:\\Windows\\System32\\coreupdater.exe', 'B']
Cyklus: ['NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\AutomaticDestinations\\9b9cdc69c1c24e2b.au
tomaticDestinations-ms', 'MAB', 'NTFS:\\System Volume Information\\DFSR\\Config\\Replica_E936046D-8F2F-444B-8F97-B9E0432F6B2A.X
ML', 'C']
Cyklus: ['NTFS:\\$MFT', 'MAB', 'NTFS:\\System Volume Information\\DFSR\\Config\\Replica_E936046D-8F2F-444B-8F97-B9E0432F6B2A.XM
L', 'C']
Cyklus: ['NTFS:\\$MFT', 'MACB', 'NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\Beth_Secret.lnk',
'MAB']
Cyklus: ['M', 'NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\AutomaticDestinations\\f01b4d95cf55d3
2a.automaticDestinations-ms', 'C', 'NTFS:\\Windows\\System32\\coreupdater.exe']
Cyklus: ['M', 'NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\AutomaticDestinations\\9b9cdc69c1c24e
2b.automaticDestinations-ms', 'C', 'NTFS:\\Windows\\System32\\coreupdater.exe']
Cyklus: ['NTFS:\\$MFT', 'A', 'NTFS:\\Windows\\System32\\coreupdater.exe', 'B']
Cyklus: ['NTFS:\\$MFT', 'MC', 'NTFS:\\Windows\\System32\\wbem\\Performance\\WmiApRpl.ini', 'A']
Cyklus: ['NTFS:\\Windows\\System32\\wbem\\Performance\\WmiApRpl.h', 'MC', 'NTFS:\\Windows\\System32\\wbem\\Performance\\WmiApRp
l.ini', 'A']
Cyklus: ['NTFS:\\Users\\Administrator\\AppData\\LocalLow\\Microsoft\\CryptnetUrlCache\\MetaData\\6BADA8974A10C4BD62CC921D13E43B
18_BEB37ABADF39714871232B4792417E04', 'AB', 'NTFS:\\Windows\\Inf\\WmiApRpl\\WmiApRpl.h', 'MC']
Cyklus: ['NTFS:\\$MFT', 'AB', 'NTFS:\\Windows\\Inf\\WmiApRpl\\WmiApRpl.h', 'MC']
Cyklus: ['NTFS:\\Users\\Administrator\\AppData\\LocalLow\\Microsoft\\CryptnetUrlCache\\MetaData\\6BADA8974A10C4BD62CC921D13E43B
18_D9817BD5013875AD517DA73475345203', 'AB', 'NTFS:\\Windows\\Inf\\WmiApRpl\\WmiApRpl.h', 'MC']
Cyklus: ['NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\28c8b86deab549a1.custo
mDestinations-ms', 'AB', 'NTFS:\\Windows\\Inf\\WmiApRpl\\WmiApRpl.h', 'MC']
Cyklus: ['NTFS:\\Users\\Administrator\\Documents\\Default.rdp', 'AB', 'NTFS:\\Windows\\Inf\\WmiApRpl\\WmiApRpl.h', 'MC']
Cyklus: ['NTFS:\\Users\\Administrator\\AppData\\Local\\Microsoft\\Terminal Server Client\\Cache\\Cache0000.bin', 'AB', 'NTF
S:\\Windows\\Inf\\WmiApRpl\\WmiApRpl.h', 'MC']
Cyklus: ['NTFS:\\$MFT', 'M', 'NTFS:\\Windows\\System32\\coreupdater.exe', 'B']
Cyklus: ['NTFS:\\$MFT', 'ACB', 'NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\AutomaticDestination
s\\1bc392b8e104a00e.automaticDestinations-ms', 'M']
Cyklus: ['NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\590aee7bdd69b59b.custo
mDestinations-ms', 'MA', 'NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\AutomaticDestinations\\1bc
392b8e104a00e.automaticDestinations-ms', 'M', 'NTFS:\\Windows\\System32\\coreupdater.exe', 'B', 'NTFS:\\Users\\Administrator\\A
ppData\\Local\\Temp\\1', 'MAC']
Cyklus: ['NTFS:\\$MFT', 'MA', 'NTFS:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\AutomaticDestinations
\\1bc392b8e104a00e.automaticDestinations-ms', 'M']
```

ĎAKUJEM ZA POZORNOSŤ