#### **Toward Graph-Based Network Traffic Analysis and Incident Investigation**

DFRWS-EU 2022 – Short Presentations

Milan Cermak

Masaryk University, Brno, Czech Republic

#### **Data Analysis and Human Brain**

## The human brain is used to perceiving the surrounding world and data in associations

- We use associations every day, so why not use them during network traffic analysis and incident investigation?
- Traditional analysis tools provide association-based analysis only in limited form or not at all
- Graph data visualization allows us to get a broader context of the analyzed data thanks to the visual aspect
- It is a commonly used technique in a criminal investigation



Paper vector created by macrovector - www.freepik.com

#### **Requirements** for Network Traffic Analysis and Incident Investigation

#### **Evaluation of Common Tools**

### When some serious incident happened in the network, we need to investigate its type, origin, impact, and spread to prevent further damage

- How did the malware get on the machine?
- Did the attacker exploit any vulnerability?
- Did the machine communicate to a malware C&C or another suspicious IP address?
- Did the machine communicate with other devices in our network? How?
- Did any device from our network communicate with the same destinations as the compromised one?

To understand the capabilities of today's tools, we have utilized <u>CyberCzech dataset</u>, selected an initial alert, and investigated it using **Wireshark**, **Arkime**, and **Brim** 

#### Wireshark

- A widely-used network protocol analyzer providing insights into network activity at a microscopic level
- De facto standard for packet trace analysis

- + Rich and detailed support of many different protocols
- + Ability to analyze all network traffic metadata
- Performance issues in analyzing large packet traces
- Limited overview of the whole packet trace
- Missing connection to other information sources

File       Eit       View Go       Capture Analyze       Statistics Telephony Wireless       Tools       Heip         Image: Comparison of the statistics Telephony Wireless       Tools       No       No       Tools       No       No       Tools       No       No       Tools       No       No<	<b>_</b> c	odd-http.pcap				-		
Image: Control         Image:	File	Edit View Go	Capture Analyze Stat	istics Telephony Wireles	is Tools H	elp		
Apply a daptary filter - CCM/>         Composition         Protocol         Length Info           No.         Time         Source         Destination         Protocol         Length Info           4         0.652749         172.16.0.122         200.121.1.131         TCP         54 (TCP Providues Regment) 80 + 10554 (ACK) Seq1.           0         0.076697         172.16.0.122         200.121.1.131         TCP         1454 [TCP Providues Regment Inot Captured] [TCP ACKed unseen segment] 80 + 10554 (ACK) Seq1.           0         0.07697         172.16.0.122         200.121.1.131         TCP         1454 [TCP Providues Retransmission] 10554 + 80 [ACK] Seq1.           0         0.128285         200.121.1.131         TCP.16.0.122         TCP         1454 [TCP Spurious Retransmission] 10554 + 80 [ACK] Seq1.           10         0.128285         200.121.1.131         TCP.16.0.122         TCP         1454 [TCP Spurious Retransmission] 10554 + 80 [ACK] Seq1.400 [Seq1.400 [	4	I 4 🛛 📕 🗋	🗙 🙆 ९ 🗢 🕾	🗿 🗄 🚍 🗐 લ, લ,	् 🎹			
No.         Three         Source         Decision         Protocil         Length Info           4         0.027540         172.16.0.122         200.121.1.131         TCP         54 [TCP Mixed update] [TCP Acked unseen segment] 80 + 10554 [ACK] Sequ- 1.05 0.070577         172.16.0.122         TCP Mixed update]         TCP Acked unseen segment] 80 + 10554 [ACK] Sequ- 1.05 0.070570         172.16.0.122         TCP Mixed update]         TCP Acked unseen segment] 80 + 10554 [ACK] Sequ- 1.05 0.070570         172.16.0.122         TCP Mixed update]         TCP Acked unseen segment] 80 + 10554 [ACK] Sequ- 1.05 0.070570         172.16.0.122         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequ- 1.05 0.070570         172.16.0.122         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequ- 1.10 0.15046         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131         TCP Acked unseen segment] 80 + 10554 [ACK] Sequel 1.0 0.15047         200.121.1.131 <t< th=""><th>A</th><th>Apply a display filter <math>&lt;</math></th><th>Ctrl-/&gt;</th><th></th><th></th><th></th><th>Expressio</th><th></th></t<>	A	Apply a display filter $<$	Ctrl-/>				Expressio	
4 6.025749       172.16.0.122       200.121.1.131       TCP       54 [TCP Mindow Update] [TCP ACked unseen segment] 80 + 10554 [ACL] segment of c.001003 segment not c.0011003 segment not c.001103 segment not c.0011003 segmen	No.	Time	Source	Destination	Protocol	Length Info		
5 0.07667     200.121.1.131     172.16.0.122     TCP     1454 [TCP Provious segment not coptured] [TCP Spurious Retransmission]       6 0.07567     172.16.0.122     200.121.1.131     172.16.0.122     TCP     1454 [TCP Provious Retransmission]     10554 + 80  ACK] Seq1.1.       9 0.122835     200.121.1.131     172.16.0.122     TCP     1454 [TCP Spurious Retransmission]     10554 + 80  ACK] Seq1.4.       9 0.122835     200.121.1.131     172.16.0.122     TCP     154 [TCP Spurious Retransmission]     10554 + 80  ACK] Seq1.4.       10 0.122835     200.121.1.131     172.16.0.122     TCP     154 [TCP Spurious Retransmission]     10554 + 80  ACK] Seq1.4.       11 0.154162     200.121.1.131     177.16.0.122     TCP     154 [TCP Spurious Retransmission]     10554 + 80 [ACK] Seq1.4.       13 0.179966     200.121.1.131     177.16.0.122     TCP     1454 [TCP Spurious Retransmission]     10554 + 80 [ACK] Seq1.4.       14 0.15915     172.1.6.0.122     200.121.1.131     TCP.     154 [TCP Spurious Retransmission]     10554 + 80 [ACK] Seq1.4.       15 0.207155     172.1.6.0.122     200.121.1.131     TCP.     1454 [1554 + 80 [ACK] Seq1.4.     1455 [1551 [120.1632]       16 0.207155     172.1.6.0.122     200.121.1.131     TCP.     1454 [15554 + 80 [ACK] Seq1.4.     1454 [1555 + 80 [ACK] Seq1.4.       16 0.2023215     200.121.1.131     TCP.		4 0.025749	172.16.0.122	200.121.1.131	TCP	54 [TCP Window Update] [TCP ACKed unseen segment] 80 → 10554 [AC	K] Seq=	
6 0.076078       172.16.0.122       200.121.131       TCP       54 (TCP Dup ACC 221) [TCP ACKed unseem segment] 80 + 10554 [ACX [Seq:30]         9 0.12030       200.121.1.131       TCP       54 (TCP Dup ACC 221) [TCP ACKed unseem segment] 80 + 10554 [ACX [Seq:30]         9 0.12030       200.121.1.131       TCP       54 (TCP Dup ACC 221) [TCP ACKed unseem segment] 80 + 10554 [ACX [Seq:30]         10 0.120310       172.16.0.122       200.121.1.131       TCP       54 (TCP Dup ACC 221) [TCP ACKed unseem segment] 80 + 10554 [ACX [Seq:30]         11 0.15452       200.121.1.131       TCP       54 (TCP Dup ACC 221) [TCP ACKed unseem segment] 80 + 10554 [ACX [Seq:30]         12 0.15450       172.16.0.122       200.121.1.131       TCP       54 (TCP Dup ACC 281) [TCP ACKed unseem segment] 80 + 10554 [ACX [Seq:30]         13 0.179960       200.121.1.131       TCP       54 (TCP Dup ACC 281) [TCP ACKed unseem segment] 80 + 10554 [ACX [Seq:30]         14 0.179915       172.16.0.122       200.121.1.131       TCP       54 [TCP Dup ACC 281] [TCP ACKed unseem segment] 80 + 10554 [ACK [Seq:30]         14 0.179915       172.16.0.122       200.121.1.131       TCP       54 [ACK [Seq:120] ACC] Seq:300 [ACK 281] [PC ACK 282] [PC ACK 281]		5 0.076967	200.121.1.131	172.16.0.122		1454 [TCP Previous segment not captured] [TCP Spurious Retransmiss	ion] 10	
7 0.102939       200.121.1.131       172.16.0.122       TCP       1434 [TCP Spurious Retransission] 10554 + 80 [ACK] Seq=1.64.1 Mine65.         9 0.128285       200.121.1.131       172.16.0.122       TCP       1434 [TCP Spurious Retransission] 10554 + 80 [ACK] Seq=1.04.1 Mine65.         10 0.128285       200.121.1.131       172.16.0.122       TCP       1434 [TCP Spurious Retransission] 10554 + 80 [ACK] Seq=1.04.1 Mine65.         11 0.15452       200.121.1.131       172.16.0.122       TCP       1454 [TCP Spurious Retransission] 10554 + 80 [ACK] Seq=1.04.1 Mine5.         12 0.154610       172.16.0.122       000.121.1.131       TCP       54 [TCP Dpx Acx 280] [TCP Acx 480 [ACK] Seq=1.08.1 Mine5.         13 0.179906       200.121.1.131       177.16.0.122       TCP       1454 [TCP Spurious Retransistion] 10554 + 80 [ACK] Seq=1.02.1 Mine5.         14 0.179715       172.16.0.122       000.121.1.131       TCP       54 80 + 10554 [ACK] Seq=1.02.1 Mine5.         19 0.20320       120.1.131       177.16.0.122       TCP       1454 10554 + 80 [ACK] Seq=1.02.1 Mine5.       160.202.1 Mine5.         19 0.228305       200.121.1.131       TCP. 1454 10554 + 80 [ACK] Seq=1.02.1 Mine5.       160.202.1 Mine5.       160.202.1 Mine5.         19 0.228305       200.121.1.131       TCP. 1454 10554 + 80 [ACK] Seq=1.02.1 Mine5.       160.202.1 Mine5.       160.202.1 Mine5.         19 0.258305 </td <td></td> <td>6 0.076978</td> <td>172.16.0.122</td> <td>200.121.1.131</td> <td></td> <td>54 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 10554 [ACK]</td> <td></td> <td></td>		6 0.076978	172.16.0.122	200.121.1.131		54 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 10554 [ACK]		
8 8.102346       1172.16.0.122       208.121.1.131       TCP       54 TCP Dup ACC 222] TCP ACked unseen segment] 80 + 10554 [ACK] Seq-1         10 0.123810       1172.16.0.122       200.121.1.131       TCP       54 TCP Dup ACC 223] TCP ACked unseen segment] 80 + 10554 [ACK] Seq-1         10 0.123810       1172.16.0.122       200.121.1.131       TCP       54 TCP Dup ACC 223] TCP ACked unseen segment] 80 + 10554 [ACK] Seq-1         11 0.15462       200.121.1.131       TCP       54 TCP Dup ACC 223] TCP ACked unseen segment] 80 + 10554 [ACK] Seq-1         12 0.15450       1172.16.0.122       200.121.1.131       TCP       54 TCP Dup ACC 224] TCP ACked unseen segment] 80 + 10554 [ACK] Seq-1         13 0.17960       200.121.1.131       TCP       54 TCP Dup ACC 224] TCP ACked unseen segment] 80 + 10554 [ACK] Seq-1         14 0.179015       1172.1.6.0.122       200.121.1.131       TCP       54 TCP Dup ACC 245 [BC ACC] Seq-1201 ACked Nime5300 Len-0         19 0.25252       200.121.1.131       TCP       54 80 + 10554 [ACK] Seq-1201 ACked Nime5300 Len-0         10 0.25355       200.121.1.131       TCP       54 80 + 10554 [ACK] Seq-1400 ACked Nime5300 Len-0         10 0.25355       200.121.1.131       TCP       54 80 + 10554 [ACK] Seq-1401 ACked Nime5300 Len-0         10 0.25355       200.201.1.131       TCP       54 80 + 10554 [ACK] Seq-1480 ACked Nime5300 Len-0         10 0.2		7 0.102939	200.121.1.131	172.16.0.122		1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=5601 Ack=1	Win=65	
9 0.12235       220.121.1.11       172.16.0.122       TCP       1434 [TCP Spurious Retransistion] 10554 + 80 [ACK] seq.7.001 Ack.1 Mine55.         10 0.123162       220.121.1.11       177.16.0.122       TCP       1434 [TCP Spurious Retransistion] 10554 + 80 [ACK] seq.1-80 + 10554 + 80 [ACK] seq.1-80 + 10553 + 1050 [ACH] seq.1-80 + 10553 [ACK] seq.1-80 + 10553 [ACK] seq.1-80 + 10553 [ACK] seq.1-80 + 10553 [ACK] seq.1-80 + 10554 + 80 [ACK] seq.1-80 + 10554 + 80 [ACK] seq.1-80 + 1056 [ACK]		8 0.102946	172.16.0.122	200.121.1.131		54 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80 → 10554 [ACK]	Seq=1	
10       0.108319       172.16.0.122       200.171.131       TCP       54       TCP Dup ACK 201       10554 - 80       ACK 15 Sequent ACK 160         11       0.10542       200.121.1.01       172.16.0.122       TCP       144       TCP Suprovs Retransmission 10554 - 80       ACK 15 Sequent ACK 160       NimeSen         13       0.17966       200.121.1.01       TCP       144       TCP Suprovs Retransmission 10554 - 80       ACK 15 Sequent ACK 160         14       0.17967       200.121.1.01       TCP       144       TCP Suprovs Retransmission 10554 - 80       ACK 15 Sequent ACK 160         15       0.207155       172.16.0.122       200.121.1.131       TCP       54       RCF Degrad ACK 15 Sequent ACK 160       Nime5300       Len-400       TCP Segment of -         16       0.207155       172.16.0.122       200.121.1.131       TCP       54 80 + 18554       ACK 15 Sequent ACK 160       Nime5300       Len-400       TCP Segment of -         18       0.232529       172.16.0.122       200.121.1.131       TCP       54 80 + 18554       ACK 15 Seque1ACK 160401       Kinne-5300       Len-400       TCP Segment of -         18       0.232529       172.16.0.122       200.121.1.131       TCP       54 80 + 18554       ACK 15 Seq-1ACK 164001       Kinne-5300       Le		9 0.128285	200.121.1.131	172.16.0.122	TCP	1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=7001 Ack=1		
110.154.02       200.121.1.11       172.156.122       TCP       1454 [TCP SpinFolds Referentiation of the set		10 0.128319	172.16.0.122	200.121.1.131	тср	54 [TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80 → 10554 [ACK]		
12 0.104.09       122.15.05.122       200.121.131       TCP       35 [1CP bap Ack 243] [ICP bap Ack 243] [ICP bap Ack 243] [ICP bap Ack 243] [ICP bap Ack 245] [I		11 0.154162	200.121.1.131	172.16.0.122	TCP	1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=8401 ACK=1	W1n=65	
130       121       111       170       120       120       121       111       170       120       1		12 0.154169	1/2.16.0.122	200.121.1.131	TCP	54 [ICP Dup ACK 2#4] [ICP ACKed unseen segment] 80 → 10554 [ACK]	Seq=1	
13       0.22130       12221301122       12221301122       100       1		13 0.179906	200.121.1.131	1/2.16.0.122	TCP	1454 [TCP Spurious Retrainsmission] 10554 + 80 [ACK] Seq=9801 ACK=1	WIN=65	
10       200.121.1.131       117.105.112       117.115.105.122       117.105.112		14 0.1/9915	200 121 1 121	172 16 0 122	TCP	54 [TCP Dup Ack 2#5] 80 → 10554 [Ack] Seq=1 Ack=11201 Win=65000	cen=0	
17 0.23221       200.122.1.131       172.16.0.122       TCP       1454 10554 = 00 [ACL] Seq=12601 ACL3 kine6335 Lem.3400 [CFP segment of _         18 0.23529       172.16.0.122       200.121.1.131       TCP       54 80 + 10554 = 00 [ACL] Seq=12601 ACL3 kine6335 Lem.3400 [CFP segment of _         18 0.23569       200.121.1.131       172.16.0.122       200.121.1.131       TCP       54 80 + 10554 [ACL] Seq=14001 ACL3 kine6335 Lem.3400 [CFP segment of _         2 0.25373       172.16.0.122       200.121.1.131       TCP       1454 10554 = 00 [ACL] Seq=14001 ACL3 kine65335 Lem.3400 [CFP segment of _         2 0.25373       172.16.0.122       200.121.1.131       TCP       1454 10554 = 00 [ACL] Seq=14001 ACL3 kine65335 Lem.3400 Lem.0         3 Prame 15: 1454 bytes on unit (11652 Dits), 1454 bytes captured (11632 Dits), 1454 bytes captured (11632 Dits), 1456 bytes captured (11632 Dits)       110001 Control Version (1160 (Onise):56:00:0010), Dit: Vmone, 42:12:13 (00:00:129:42:12:13)         3 Internet Protocol Version A, scr: 200.121.1.131, Dit: 172.16.0.122       Vmannission Control Protocol, Scr Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400         Source Port: 1855       Destination Port: 80       [CrP Segment Lem: 1400]       Sequence number: 11201         [CrP Segment Lem: 1400]       Sequence number: 11201       (relative sequence number)]       Ackschwaledgement number: 12001         [CrD Segment C mumber: 1200]       [Crelative sequence number]       [Ack P, N, -:0		15 0.207145	172 16 0 122	200 121 1 131	TCP	54 80 - 10554 [ACK] Seg=11201 ACK=1 Win=63090 Len=0	enc or	
18 0.222.0       172.16.0.122       200.121.1.31       TCP       54 80 + 10554 [CK] Seq.1 Act. 14001 Kin-63000 Lenned         18 0.225.20       172.16.0.122       200.121.1.31       TCP       54 80 + 10554 [CK] Seq.1 Act. 14001 Kin-63000 Lenned         10 0.258.55       200.121.1.131       172.16.0.122       TCP       1454 10554 - 80 [CK] Seq.1 Act. 14001 Kin-63000 Lenned         20 0.258.75       122.16.0.122       200.111.1.131       TCP       54 80 + 10554 [CK] Seq.1 Act. 15401 Kin-63000 Lenned         > Frame 15: 1454 bytes on wire (11612 bits), 1454 bytes captured (11632 bits)       >          > Internet Frotocol Version 4, 5c: 200.111.1.131, 05: 172.16.0.122       >         Y Transission Control Protocol, Src Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400       >         Source Port: 10554       Destination Port: 80          [Stream index: 0]       [relative sequence number)       [Ket sequence number]         [Ket sequence number: 12601       (relative sequence number)]       Acknowledgement number: 1261         [0011       = Header Length: 20 bytes (5)		17 0 232621	200 121 1 131	172 16 0 122	TCP	1454 19554 - 88 [ACK] Seg=12681 Ack=1 Win=65535 Len=1498 [TCD com	ent of	
19 0.258365       200.122.1.131       172.16.0.122       TCP       1454 19554 = 00 [ACL] Seq-14001 Acts! Mine5335 ten:1400 [TCP segment of _         20 0.258373       172.16.0.122       200.121.1.131       TCP       54 80 + 18554 = 80 [ACL] Seq-14001 Acts! Mine5335 ten:1400 [TCP segment of _         5 Prane 15: 1454 bytes on unic (11632 bits).       1545 bytes on unic (11632 bits).       1545 bytes on unic (11632 bits).         5 Internet TU, Src: Vmare_c00001 (00:50:55:c00:001), Dst: Vmare_c2:12:13 (00:0c:29:42:12:13)       1516-0.122         7 Internet Torocol Version A, src: 200.121.1.131, Ost: 172.16.0.122       vmare_c2:12:13.10       120.10.133.0         9 Internet Torocol Version A, src: 200.121.1.131, Ost: 172.16.0.122       vmare_c2:12:13.10       120.10.133.0         9 Surgence number: 11281       (relative sequence number)       160.00.00.00.00.00.00.00.00.00.00.00.00.0		18 0.232629	172.16.0.122	200.121.1.131	TCP	54 80 → 10554 [ACK] Seg=1 Ack=14001 Win=63000 Len=0	enc or	
20 0.258373       172.16.0.122       200.121.1.131       TCP       54 80 - 18554 [ACK] Seq=1 Ack=15401 Win=63000 Len=0         > Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)       Ethernet I7, Src: Vmare q.212.1.213 (00:00:23942:121130)         > Internet Protocol Version 4, Src: 200.121.1.131, DSt: 172.16.0.122       Yman internet Protocol Version 4, Src: 200.121.1.131, DSt: 172.16.0.122         > Internet Protocol Version 4, Src: 200.121.1.131, DSt: 172.16.0.122       Yman internet Protocol Version 4, Src: 200.121.1.131, DSt: 172.16.0.122         > Transmission Port: 100       Source Port: 10554       Destination Port: 100         Sequence number: 11201       (relative sequence number)       [Ket Sequence number: 11206]         I(PL Sequence number: 11201       (relative sequence number)]       Acknowledgeent number: 1201         0000       07 20 DSE 00 So v1 Sc: 20 00 e1 2 ce bet 56 01       TP         0101		19 0.258365	200.121.1.131	172.16.0.122	TCP	1454 10554 → 80 [ACK] Seg=14001 Ack=1 Win=65535 Len=1400 [TCP segm	ent of	
> Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) > Ethernet II, Src: Ymware_c000010, 000:50:56:c0:00010, Dat: Ymware_42:12:13 (00:0c:20:42:12:13) > Internet Froctocol Version A, Src: 200:121:10.50, 122 Y Transmission Control Protocol, Src Port: 10554, Dat Port: 80, Seq: 11201, Ack: 1, Len: 1400 Source Port: 10554 Destination Port: 80 [Stream index: 0] [IfCP Segment Len: 1400] Sequence number: 12601 (relative sequence number) [Mext sequence number: 12601 (relative sequence number)] Acknowledgment number: 12601 (relative sequence number)] Acknowledgment number: 12601 (relative sequence number) 00200 007 a 0020 007 a 00200 00 ar 55 as 08 as 2 e2 ee bf 50 10 20007 for 15 to 60 08 02 47 rd 82 55 25 21: 0000 71 \$5 06 03 39 34 54 77 rd 84 c5 13 34 78 35 25 21: 0000 71 \$5 06 53 03 34 44 559 77 49 70 65 132 44 37 VSB-88 45 21: 0000 31 56 73 55 65 61 33 46 44 55 25 21: 0000 73 56 75 65 59 77 54 62 58 66 64 65 25 21: 0000 73 56 77 55 77 54 65 28 66 64 65 20 20: 0000 78 67 75 74 65 30 73 55 77 80 78 65 77 80 78 65 77 80 78 77 80 78 65 78 78 78 78 78 78 78 78 78 78 78 78 78		20 0.258373	172.16.0.122	200.121.1.131	TCP	54 80 → 10554 [ACK] Seg=1 Ack=15401 Win=63000 Len=0		
0010	> E > I ~ T	Ethernet II, Src: Internet Protocol Transmission Cont Source Port: 10 Destination Por [Stream index: [TCP Segment L Sequence numbe] [Next sequence Acknowledgment	Vmware_c0:00:01 (00 Version 4, Src: 200 rol Protocol, Src Po 2554 en: 1400] r: 11201 (relativ number: 12601 (r number: 1 (relat	:50:56:c0:00:01), Dst .121.1.131, Dst: 172. rt: 10554, Dst Port: e sequence number) elative sequence numb ive ack number)	: Vmware_42 16.0.122 80, Seq: 11 er)]	::12:13 (00:0c:29:42:12:13) 201, Ack: 1, Len: 1400		
0020         007         20         02         00         7         02         00         7         02         00         7         02         00         7         02         00         7         02         00         7         02         00         7         02         00         02         00         7         02         00         02         00         02         00         02         00         02         00         02         00         02         00         02         00         02         00         02		0101 = He	ader Length: 20 byte	s (5)				
00070 2/ HE DE 22 D2 H2 /2 HE DU D2 30 22 /0 28 5/ /a WLISECKIN MICHERARXZ	002 003 004 005 006 007 008	20         00         7a         29         3a         00           30         ff         ff         bc         5e         00           30         ff         ff         bc         3e         6f         3f           70         33         56         75         35         56         70         78         4c         44         4d         74           30         63         66         66         66         66         56         76	50         a7         5c         30         08         e2           00         42         4f         78         42         56           34         54         77         48         4c         71           55         6e         59         73         46         2b           61         33         4d         44         59         77           38         6b         2f         75         42         68           35         6a         77         77         42         68	e2 ee bf 50 10 · 21 35 6a 45 52 52 · · · ^ 46 51 34 78 35 qZici 67 6c 44 47 4c abF0 970 63 32 44 3Vu5 38 6a 48 6d 30 xLDM 56 4c 6f 6c 41 cftc	P·\ 01 BO xBV5jEl 94Tw HLqFQ4: wUnY sF+g1Di ea3M DYwIpc; t8k/ uBh8jHr 15jw wL/VLO	2. 18 14 15 15 10 16 16 16		
	009			32 /0 30 3/ /d WLI5	ссун шсокрхі	n2		

Wireshark: https://www.wireshark.org/

#### **Arkime (formerly Moloch)**

- A large-scale, open-source, indexed packet capture and search tool with a web interface
- + Indexed data storage for fast data analysis
- + Extraction of various information from network sessions and other metadata
- + Basic statistics of extracted data
- + Export of selected connections as packet traces
- No alerts correlation
- Missing connection to other information sources

🖣 See	sions SPIVi	ew SPIGraph	n Connections Fil	es Stats ⊦	listory Settings U	sers						v2.7.1 ?
A Searc	h										8	K Search
D Last P	iour Sta	rt 2021/03/01	16:12:03 N N	End 2021	/03/01 17:12:03	H H Bour	nding Last Pa	icket Inter	val Auto			
50 per page	. a. c	1 2 3 > »	<ul> <li>Showing 1 - 50 of 148</li> </ul>	entries								_
00						Destrate	Puter Data hut	a line Per				
50				QC		Packets	bytes Data byt	Lines Bars				
00 00												- 1
50												
0												I.
20	21/03/01 6:15:00	2021/03/01 16:20:00	2021/03/01 202 16:25:00 16	1/03/01 1:30:00	2021/03/01 2021/ 16:35:00 16:4	03/01 2 0:00	021/03/01 16:45:00	2021/03/01 16:50:00	2021/03/01 16:55:00	2021/03/01 17:00:00	2021/03/01 17:05:00	2021/03/01 17:10:00
		Stop Time	© Src IP / Country	© Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Arkime Node	Info		
tcp	2021/03/01	2021/03/01	93.174.93.123	46426	45.58.43.9	9569	3	0 162	ubuntu2004			
tcp	2021/03/01 17:11:06	2021/03/01 17:11:06	185.156.73.57	53823	45.58.43.9	52926	3	0 162	ubuntu2004			
icmp6	2021/03/01 17:11:05	2021/03/01 17:11:07	fe80::e86:1000:df5f:9d 00	0	ff02::1:ff00:62c6	0	3	96 258	ubuntu2004			
icmp6	2021/03/01 17:11:05	2021/03/01 17:11:07	fe80::e86:1000:df5f:9d 00	0	ff02::1:ff00:a7e3	0	3	96 258	ubuntu2004			
icmp6	2021/03/01	2021/03/01	fe80::e86:1000:df5f:9d	0	ff02::1:ff00:e2ce	0	3	96 258	ubuntu2004			
icmp6	2021/03/01	2021/03/01	2607:f170:34:10::7c0	0	ff02::1:ff00:1	0	1	32 86	ubuntu2004			
icmp6	2021/03/01	2021/03/01	fe80::e86:1000:df5f:9d	0	ff02::1:ff00:106c	0	3	96 258	ubuntu2004			
icmp6	2021/03/01	2021/03/01	fe80::e86:1000:df5f:9d	0	ff02::1:ff00:c440	0	3	96 258	ubuntu2004			
icmp6	2021/03/01	2021/03/01	2607:f170:34:13::670	0	ff02::1:ff00:1	0	1	32 86	ubuntu2004			
icmp6	2021/03/01	2021/03/01 17:11:02	fe80::e86:1000:df5f:9d	0	ff02::1:ff00:6d02	0	3	96 258	ubuntu2004			
icmp6	2021/03/01	2021/03/01	fe80::e86:1000:df5f:9d	0	ff02::1:ff00:cbda	0	3	96	ubuntu2004			

Arkime: https://arkime.com/

#### Brim

- An open-source desktop application combining Wireshark and Zeek (<u>https://zeek.org/</u>) network security monitor
- + Utilization of a Zeek to extract relevant information
- + Indexed data storage for fast data analysis
- + Alerts correlation (Suricata or external source)
- + Basic statistics of extracted data
- + Export of selected connections as packet traces
- Custom query language
- Limited visualizations
- Limited connection to other information sources



Brim: https://www.brimsecurity.com/

#### **Graph-Based Analysis of Network Traffic Data**

#### **Representation of Network Traffic Data**



- Initial version was proposed by <u>Niese</u> and further developed by <u>Leichtnam et al.</u>
- We have further developed these proposals and simplified them to ease data understanding
- Host a device with IP address observed in the network traffic capture
- Host-data data related to the host extracted from network traffic (hostname, certificate, ...)
- Connection information about individual network connections (statistics, flags, ...)
- Application application data extracted from the connection (DNS, HTTP, TLS, ...)
- All edges should be directional to ease analysis, but reverse processing could be possible

#### **Granef Toolkit**



- Demonstration of the new approach to exploratory network traffic data analysis based on associations stored in a graph database
- The toolkit's core consists of a scalable graph database Dgraph that stores transformed information from network traffic extracted by Zeek network security monitor
- Modules are implemented as Docker containers
- Custom Python scripts control all modules to ease toolkit setup and usage
- Web interface visualizes data as an interactive relationship diagram

#### **Interactive Data Exploration**

- The analyst can use predefined queries or custom DQL queries (Dgraph Query Language)
- The interactive relationship visualization allows the analyst to get details about any selected node, go into the graph's depth, and gain new observations
- Various types of attacks and anomalies can be spotted at first glance based on visual patterns

```
{getConn(func: allof(host.ip, cidr, "192.168.0.0/16"))
name : host.ip
host.originated @filter(eq(connection.proto, "tcp"))
    expand(Connection)
    connection.produced {
        expand(_all_)
        files.fuid { expand(File) }
    }
    ~host.responded { responded_ip : host.ip }
}
```

Regard x +	× - B ×
← → C △ © 127.0.0.1	🕁 🎯 Anonymni 🚦
Granef – Graph-Based Network Forensics	٥
Connection Overview Custom Query	
Connection search	
Source IP address (or CIDP): 10.02.15 Destination IP address (or CIDP): 34102136.180	
Timestamp from: 17.09.2021 12:14	
GET YAN SET CHARL	

#### **Towards Unified Analysis of Data Related to the Incident Investigation**

#### **Unified Data Analysis**

#### General incident information and OSINT data can be simply represented as graph data (as it is possible, for example, in the <u>Maltego</u> tool)

- Modern GraphQL API allows us to obtain various data from external sources directly in a format suitable for connection to a graph database
- It is also possible to link other primary data sources, such as alerts, host data, threat intelligence, etc. (if they are represented as a graph)
- The proposed approach enables us to define queries and interactively browse various data in a single graphical environment:

check the process tree that originated analyzed connection; search for IOCs and linked data; investigate network communications, disk records, account transactions, and phone calls in a single database query

#### This represents the main goal of our research!

#### Conclusion

- Graph-based analysis follows the typical way of human thinking and perception of the characteristics of the surrounding world
- The presented approach is not only the new method of network data storage and analysis, but it is also a shift of mindset that allows us to perceive network traffic in a new way
- We have introduced an open-source Granef toolkit to demonstrate exploratory network traffic analysis based on associations stored in a graph database: <u>https://granef.csirt.muni.cz</u>
- The modern GraphQL API offers great potential to connect various data related to an incident investigation

# Check granef.csirt.muni.cz to get more information about Granef and our research!

Feel free to contact me also at <u>cermak@ics.muni.cz</u>



Sharing and Automation for Privacy Preserving Attack Neutralization



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418.