Intro to NIST and Incident Response

Presented by: Albert Morris, Andy Tang, Amber Nicole, & David Sanchez

CIS 4810

The Digital Forensics Process

1. Search Authority: warrant, subpoena, or even consent.
2. Chain of Custody: essential to maintain integrity
3. Imaging/Hashing Function: Forensic image duplicating original(Read only)
4. Validated Tools: Document tool testing + validations
5. Repeatability(Quality Analysis): Collection of practices + procedures throughout the whole forensic process helping guarantee accuracy of findings
6. Analysis: Timeline, breaking encryption, connect the dots….
7. Reporting: Know your audience! Executive summary, list items examined, methods + tools used, conclusion, relevant exhibits
8. Possible Expert Presentation: Present to judge or jury


Our Incident Response Plan
goes something like this...
HELP!
HELP!

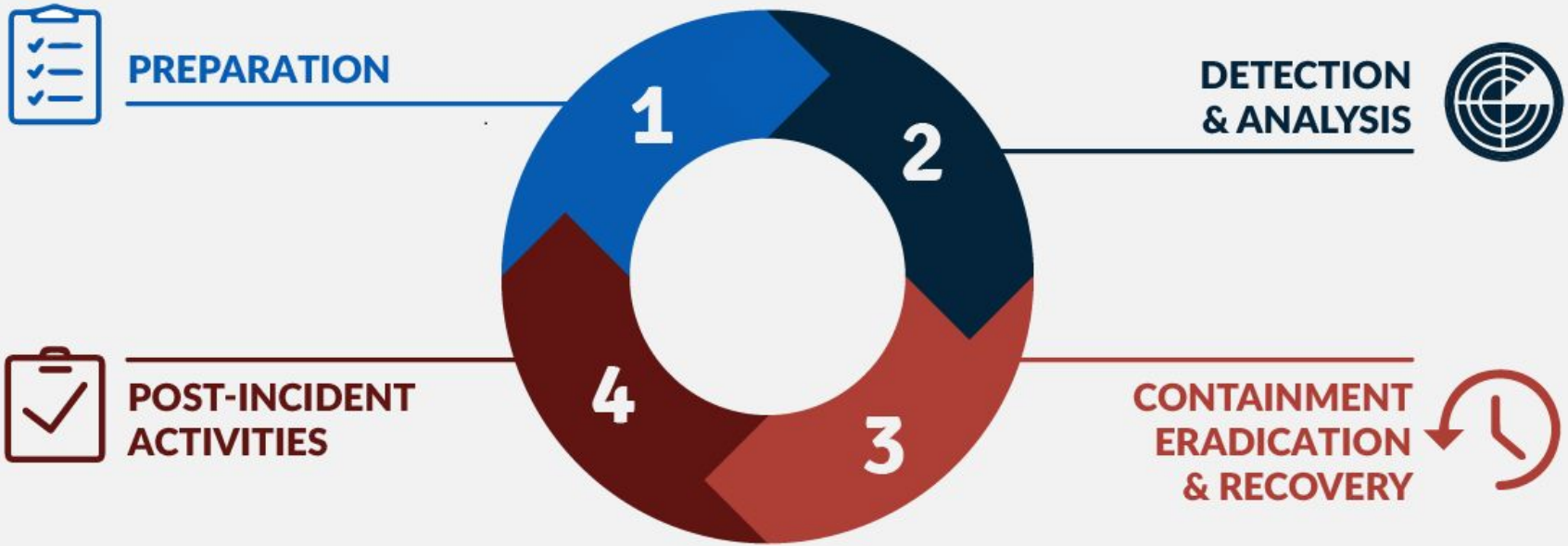
The National Institute of Standards and Technology (NIST)

- Establishes general guidelines for compliance
- Helps secures organization's infrastructure
- NIST Special Publication 800 - All Computer Security Info
  - Ex. IR Cycle is actually:
    - **NIST SP 800-61**

JOBS

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The Incident Response Lifecyle



www.blog.eLearnSecurity.com | Info source: NIST Computer Security Incident Handling Guide

Volatile vs Non-Volatile

Non-Volatile Memory:

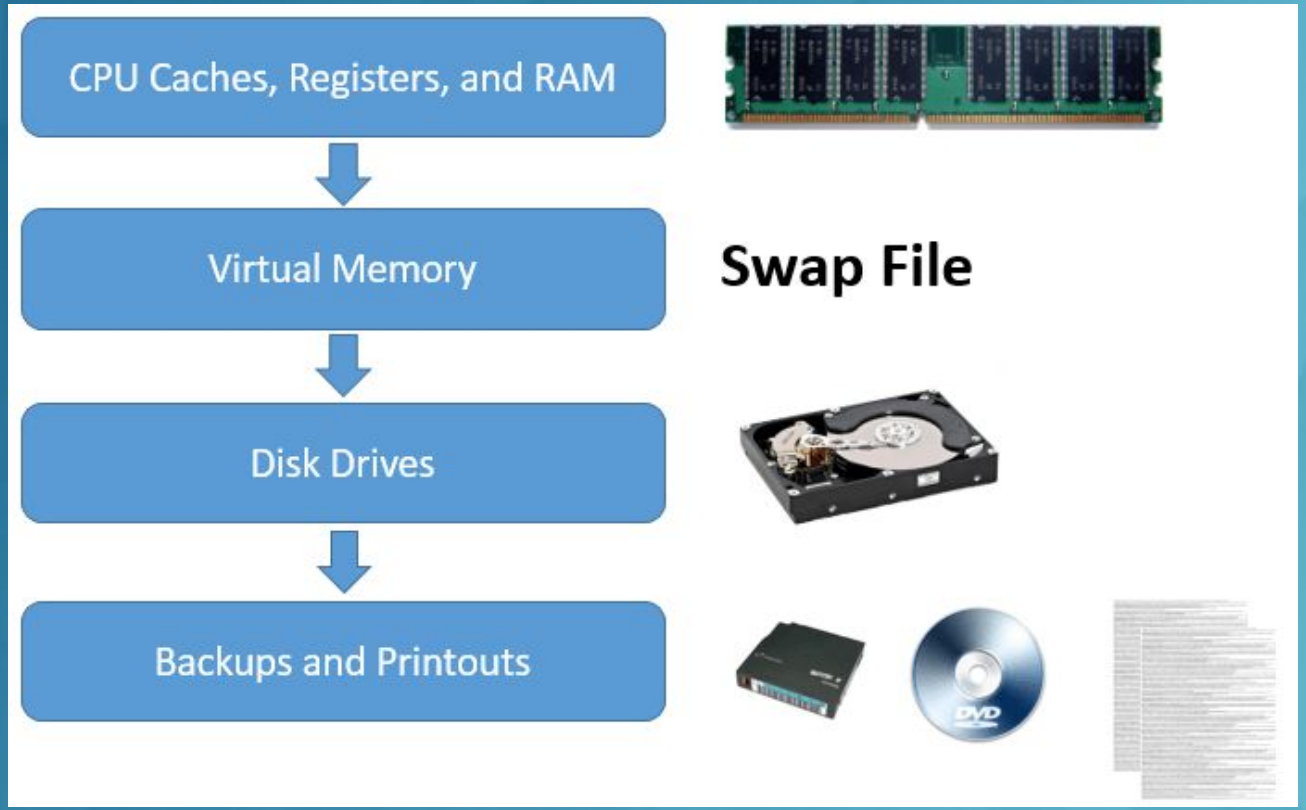
Ex. HDD, SSD, CD, DVD, etc.

Volatile Data:

Ex. RAM, pagefiles(win), swap(linux), caches, processes, etc.

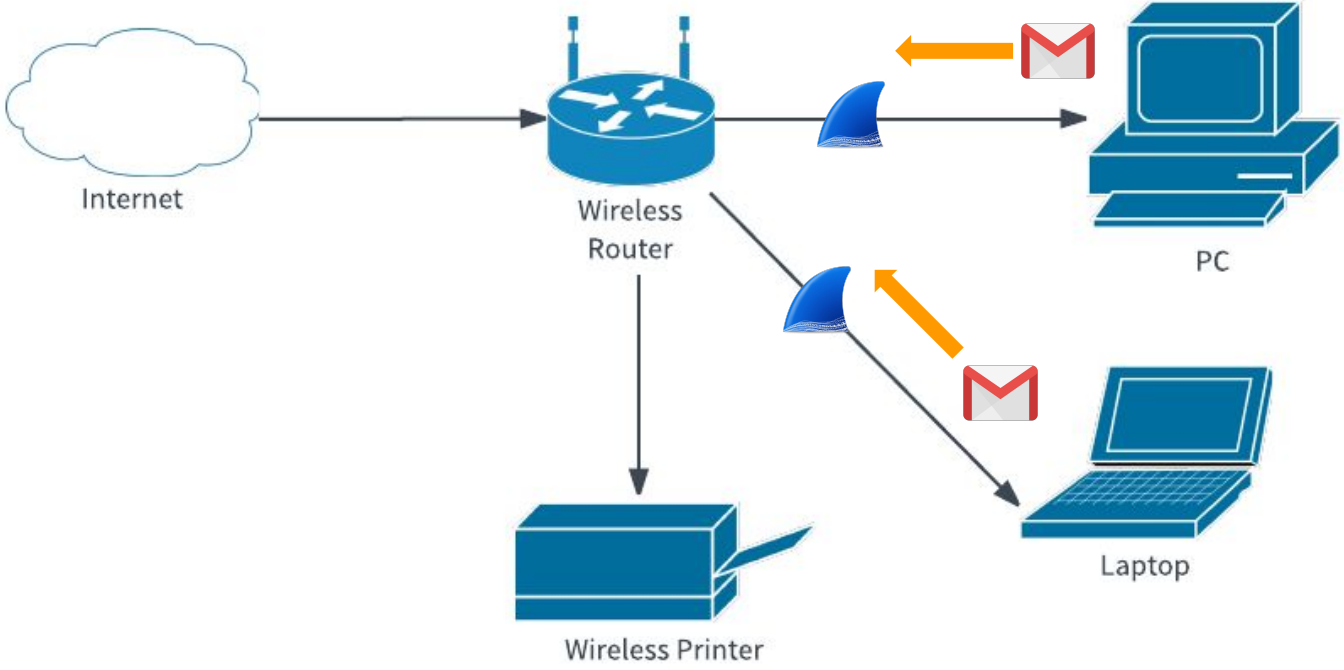
Random Access Memory (RAM): not sequential, providing CPU the necessary speed to load your program

Order of Volatility



https://blogs.getcertifiedgetahead.com/cfr-and-order-of-volatility/

WIRESHARK



time	Source	Destination	Protocol	des_port	Info
17:00:33.238957	10.7.15.101	89.238.68.194	SMTP	25	C: MAIL FROM:<fdrake@acm.org
17:00:33.238243	89.238.68.194	10.7.15.101	SMTP	49168	S: 250-vm194.documentfounda
17:00:33.067699	89.238.68.194	10.7.15.101	TCP	49168	25 → 49168 [ACK] Seq=62 Ack=
17:00:33.067597	10.7.15.101	89.238.68.194	SMTP	25	C: EHLO acm.org
17:00:33.067061	89.238.68.194	10.7.15.101	SMTP	49168	S: 220 vm194.documentfounda
17:00:32.897062	10.7.15.101	199.89.1.120	TCP	25	49163 → 25 [ACK] Seq=77 Ack=
17:00:32.896786	199.89.1.120	10.7.15.101	TCP	49163	25 → 49163 [FIN, PSH, ACK]
17:00:32.889785	10.7.15.101	10.7.15.1	DNS	53	Standard query 0x41e8 A mx2
17:00:32.885398	10.7.15.101	89.238.68.194	TCP	25	49168 → 25 [ACK] Seq=1 Ack=
17:00:32.885126	10.7.15.1	10.7.15.101	DNS	50685	Standard query response 0xd
17:00:32.884962	89.238.68.194	10.7.15.101	TCP	49168	25 → 49168 [SYN, ACK] Seq=0
17:00:32.857588	10.7.15.101	10.7.15.1	DNS	53	Standard query 0x40bc A smtp
17:00:32.856824	10.7.15.1	10.7.15.101	DNS	59663	Standard query response 0xa
17:00:32.847639	10.7.15.101	131.252.210.177	TCP	25	49167 → 25 [ACK] Seq=89 Ack=
17:00:32.847306	131.252.210.177	10.7.15.101	TCP	49167	25 → 49167 [FIN, PSH, ACK]
17:00:32.830536	10.7.15.101	10.7.15.1	DNS	53	Standard query 0x22bc A mx2
17:00:32.828259	10.7.15.101	104.17.79.191	TCP	25	49169 → 25 [SYN] Seq=0 Win=
17:00:32.827860	10.7.15.1	10.7.15.101	DNS	54288	Standard query response 0x6
17:00:32.825756	10.7.15.1	10.7.15.101	DNS	53237	Standard query response 0xf

MyDoom

What is it?

- Worm from 2004
- 1 in 12 emails at its peak
- Estimated $38 billion in damages
- Still exists today (different versions)
- **DDoS:**
  a. www.sco.com on Feb 1st, 2004
  b. www.microsoft.com on Feb 3rd, 2004

Two methods of spreading:

1. KaZaA
2. Email Spamming

Possible Filenames (KaZaA):

- winamp5.exe
- activation_crack.pif
- office_crack.bat

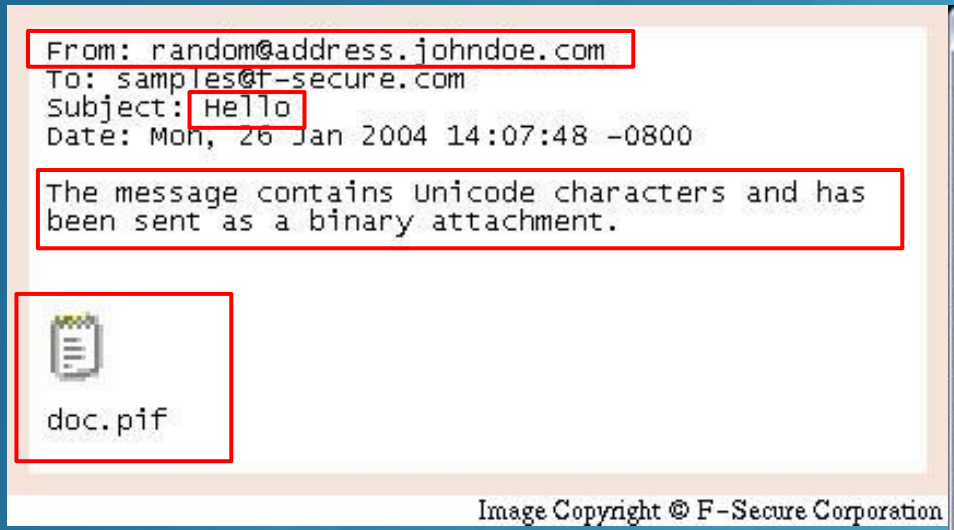
MyDoom Email Spamming

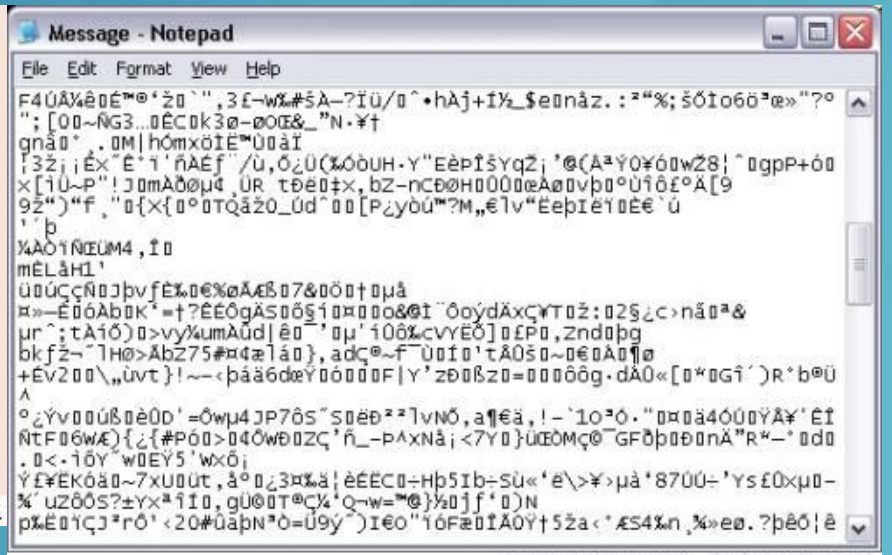
Characteristics:

- Sender address is spoofed
- Disguised as an error message
- Contains an attachment with randomly chosen name
- Creates a backdoor

Ignores:

- **Mail domains such as:** gov, mil, berkeley, google
- **Recipients such as:** bugs, help, info, postmaster, webmaster, admin, support





Demo

time	Source	Destination	Protocol	des_port	Info
17:00:33.238957	10.7.15.101	89.238.68.194	SMTP	25	C: MAIL FROM:<fdrake@acm.org
17:00:33.238243	89.238.68.194	10.7.15.101	SMTP	49168	S: 250-vm194.documentfounda
17:00:33.067699	89.238.68.194	10.7.15.101	TCP	49168	25 → 49168 [ACK] Seq=62 Ack=
17:00:33.067597	10.7.15.101	89.238.68.194	SMTP	25	C: EHLO acm.org
17:00:33.067061	89.238.68.194	10.7.15.101	SMTP	49168	S: 220 vm194.documentfounda
17:00:32.897062	10.7.15.101	199.89.1.120	TCP	25	49163 → 25 [ACK] Seq=77 Ack=
17:00:32.896786	199.89.1.120	10.7.15.101	TCP	49163	25 → 49163 [FIN, PSH, ACK]
17:00:32.889785	10.7.15.101	10.7.15.1	DNS	53	Standard query 0x41e8 A mx2
17:00:32.885398	10.7.15.101	89.238.68.194	TCP	25	49168 → 25 [ACK] Seq=1 Ack=
17:00:32.885126	10.7.15.1	10.7.15.101	DNS	50685	Standard query response 0xd
17:00:32.884962	89.238.68.194	10.7.15.101	TCP	49168	25 → 49168 [SYN, ACK] Seq=0
17:00:32.857588	10.7.15.101	10.7.15.1	DNS	53	Standard query 0x40bc A smtp
17:00:32.856824	10.7.15.1	10.7.15.101	DNS	59663	Standard query response 0xa
17:00:32.847639	10.7.15.101	131.252.210.177	TCP	25	49167 → 25 [ACK] Seq=89 Ack=
17:00:32.847306	131.252.210.177	10.7.15.101	TCP	49167	25 → 49167 [FIN, PSH, ACK]
17:00:32.830536	10.7.15.101	10.7.15.1	DNS	53	Standard query 0x22bc A mx2
17:00:32.828259	10.7.15.101	104.17.79.191	TCP	25	49169 → 25 [SYN] Seq=0 Win=
17:00:32.827860	10.7.15.1	10.7.15.101	DNS	54288	Standard query response 0x6
17:00:32.825756	10.7.15.1	10.7.15.101	DNS	53237	Standard query response 0xf

smtp.data.fragment

Expression...

time	Source	Destination	Protocol	src_port	des_port	Info
17:00:36.157647	10.7.15.101	88.99.190.237	SMTP/…	49170	25	from: "Post Office" <postmaster@documentfo
17:00:48.507920	10.7.15.101	209.85.144.27	SMTP/…	49186	25	from: "Returned mail" <postmaster@translat
17:01:04.270405	10.7.15.101	209.85.144.27	SMTP/…	49210	25	from: "Returned mail" <postmaster@translat
17:01:04.694630	10.7.15.101	64.147.108.50	SMTP/…	49209	25	from: "Mail Delivery Subsystem" <noreply@p
17:01:10.504836	10.7.15.101	185.70.40.103	SMTP/…	49211	25	from: brian.kelk@cl.cam.ac.uk, subject: Ma
17:01:22.307739	10.7.15.101	173.228.157.40	SMTP/…	49219	25	from: "Mail Delivery Subsystem" <noreply@p
17:01:23.210796	10.7.15.101	108.177.104.27	SMTP/…	49220	25	from: "Returned mail" <postmaster@translat
17:01:23.320369	10.7.15.101	116.203.90.47	SMTP/…	49221	25	from: "Post Office" <postmaster@apache.org
17:01:26.697898	10.7.15.101	185.70.40.102	SMTP/…	49224	25	from: brian.kelk@cl.cam.ac.uk, subject: Ma
17:01:39.929847	10.7.15.101	64.233.177.27	SMTP/…	49230	25	from: "Returned mail" <postmaster@translat
17:01:43.044508	10.7.15.101	34.199.147.133	SMTP/…	49234	25	from: "Post Office" <postmaster@apache.org
17:01:45.849321	10.7.15.101	173.228.157.42	SMTP/…	49240	25	from: "Mail Delivery Subsystem" <noreply@p
17:01:55.601723	10.7.15.101	64.233.177.26	SMTP/…	49246	25	from: "Returned mail" <postmaster@translat
17:01:58.693910	10.7.15.101	207.244.88.150	SMTP/…	49247	25	from: "Post Office" <postmaster@apache.org
17:02:10.500302	10.7.15.101	64.147.108.55	SMTP/…	49248	25	from: "Mail Delivery Subsystem" <noreply@p
17:02:17.956165	10.7.15.101	185.70.40.103	SMTP/…	49250	25	from: brian.kelk@cl.cam.ac.uk, subject: Ma
17:02:28.237144	10.7.15.101	173.228.157.41	SMTP/…	49255	25	from: "Mail Delivery Subsystem" <noreply@p
17:02:45.513709	10.7.15.101	173.228.157.39	SMTP/…	49257	25	from: "Mail Delivery Subsystem" <noreply@p
17:03:01.885655	10.7.15.101	64.147.108.51	SMTP/…	49259	25	from: "Mail Delivery Subsystem" <noreply@p
17:03:17.510275	10.7.15.101	64.147.108.52	SMTP/…	49261	25	from: "Mail Delivery Subsystem" <noreply@p
17:03:34.255986	10.7.15.101	185.70.40.103	SMTP/…	49262	25	from: "Automatic Email Delivery Software"
17:03:50.463434	10.7.15.101	185.70.40.102	SMTP/…	49267	25	from: "Automatic Email Delivery Software"
17:04:28.483141	10.7.15.101	185.70.40.103	SMTP/…	49271	25	from: "Automatic Email Delivery Software"

smtp and ip contains "MAIL FROM:"

time	Source	Destination	Protocol	src_port	des_port	Info
17:01…	10.7.15.101	192.254.190.1…	SMTP	49217	25	C: MAIL FROM:<noreply@onlineconnections.com.au>
17:01…	10.7.15.101	185.70.40.102	SMTP	49224	25	C: MAIL FROM:<brian.kelk@cl.cam.ac.uk>
17:01…	10.7.15.101	209.249.171.1…	SMTP	49225	25	C: MAIL FROM:<postmaster@theriver.com>
17:01…	10.7.15.101	209.249.171.1…	SMTP	49228	25	C: MAIL FROM:<postmaster@theriver.com>
17:01…	10.7.15.101	192.254.190.1…	SMTP	49227	25	C: MAIL FROM:<noreply@onlineconnections.com.au>
17:01…	10.7.15.101	64.233.177.27	SMTP	49230	25	C: MAIL FROM:<postmaster@translate.org.za>
17:01…	10.7.15.101	34.199.147.133	SMTP	49234	25	C: MAIL FROM:<postmaster@apache.org>
17:01…	10.7.15.101	173.228.157.42	SMTP	49240	25	C: MAIL FROM:<noreply@pobox.com>
17:01…	10.7.15.101	216.97.88.9	SMTP	49235	25	C: MAIL FROM:<MAILER-DAEMON@unicode.org>
17:01…	10.7.15.101	64.233.177.26	SMTP	49246	25	C: MAIL FROM:<postmaster@translate.org.za>
17:01…	10.7.15.101	216.97.88.9	SMTP	49245	25	C: MAIL FROM:<MAILER-DAEMON@unicode.org>
17:01…	10.7.15.101	207.244.88.150	SMTP	49247	25	C: MAIL FROM:<postmaster@apache.org>
17:02…	10.7.15.101	64.147.108.55	SMTP	49248	25	C: MAIL FROM:<noreply@pobox.com>
17:02…	10.7.15.101	185.70.40.103	SMTP	49250	25	C: MAIL FROM:<brian.kelk@cl.cam.ac.uk>
17:02…	10.7.15.101	173.228.157.41	SMTP	49255	25	C: MAIL FROM:<noreply@pobox.com>
17:02…	10.7.15.101	173.228.157.39	SMTP	49257	25	C: MAIL FROM:<noreply@pobox.com>
17:03…	10.7.15.101	64.147.108.51	SMTP	49259	25	C: MAIL FROM:<noreply@pobox.com>
17:03…	10.7.15.101	64.147.108.52	SMTP	49261	25	C: MAIL FROM:<noreply@pobox.com>
17:03…	10.7.15.101	185.70.40.103	SMTP	49262	25	C: MAIL FROM:<postmaster@protonmail.ch>
17:03…	10.7.15.101	173.228.157.53	SMTP	49266	25	C: MAIL FROM:<noreply@pobox.com>
17:03…	10.7.15.101	185.70.40.102	SMTP	49267	25	C: MAIL FROM:<postmaster@protonmail.ch>
17:04…	10.7.15.101	185.70.40.103	SMTP	49271	25	C: MAIL FROM:<postmaster@protonmail.ch>
17:04…	10.7.15.101	207.244.88.150	SMTP	49274	25	C: MAIL FROM:<MAILER-DAEMON@openoffice.org>

smtp and ip contains "Subject:"

time	Source	Destination	Protocol	src_port	des_port	Info
17:00…	10.7.15.101	88.99.190.237	SMTP	49170	25	C: DATA fragment, 1460 bytes
17:00…	10.7.15.101	209.85.144.27	SMTP	49186	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	209.85.144.27	SMTP	49210	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	64.147.108.50	SMTP	49209	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	185.70.40.103	SMTP	49211	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	173.228.157.40	SMTP	49219	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	108.177.104.27	SMTP	49220	25	C: DATA fragment, 43 bytes
17:01…	10.7.15.101	116.203.90.47	SMTP	49221	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	185.70.40.102	SMTP	49224	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	64.233.177.27	SMTP	49230	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	34.199.147.133	SMTP	49234	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	173.228.157.42	SMTP	49240	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	64.233.177.26	SMTP	49246	25	C: DATA fragment, 1460 bytes
17:01…	10.7.15.101	207.244.88.150	SMTP	49247	25	C: DATA fragment, 1460 bytes
17:02…	10.7.15.101	64.147.108.55	SMTP	49248	25	C: DATA fragment, 1460 bytes
17:02…	10.7.15.101	185.70.40.103	SMTP	49250	25	C: DATA fragment, 1460 bytes
17:02…	10.7.15.101	173.228.157.41	SMTP	49255	25	C: DATA fragment, 1460 bytes
17:02…	10.7.15.101	173.228.157.39	SMTP	49257	25	C: DATA fragment, 1460 bytes
17:03…	10.7.15.101	64.147.108.51	SMTP	49259	25	C: DATA fragment, 1460 bytes
17:03…	10.7.15.101	64.147.108.52	SMTP	49261	25	C: DATA fragment, 52 bytes
17:03…	10.7.15.101	185.70.40.103	SMTP	49262	25	C: DATA fragment, 1460 bytes
17:03…	10.7.15.101	185.70.40.102	SMTP	49267	25	C: DATA fragment, 1460 bytes
17:04…	10.7.15.101	185.70.40.103	SMTP	49271	25	C: DATA fragment, 1460 bytes

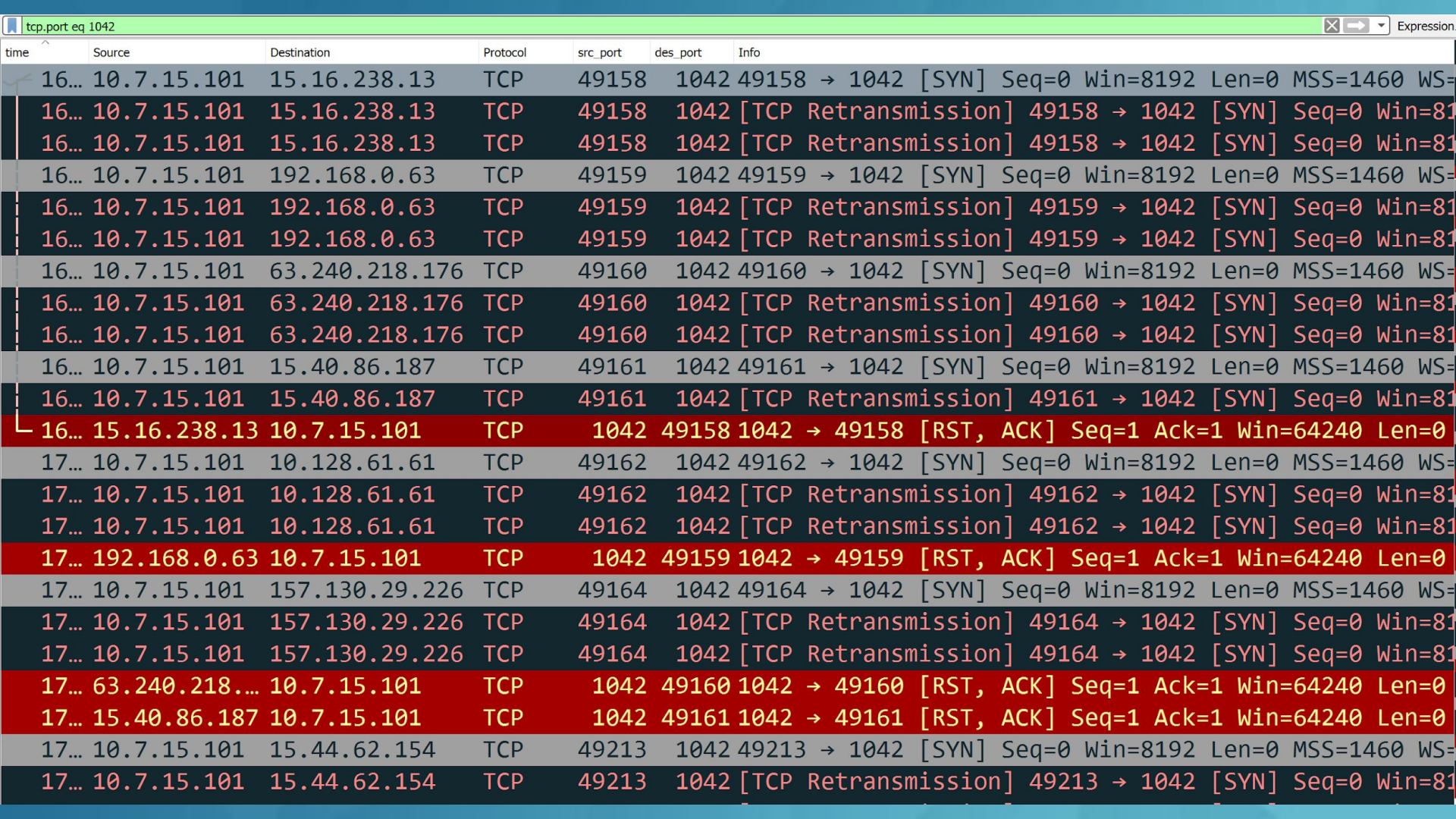
```
DATA
354 End data with <CR><LF>.<CR><LF>
From: brian.kelk@cl.cam.ac.uk
To: btitze@protonmail.ch
Subject: Mail System Error - Returned Mail
Date: Mon, 15 Jul 2019 17:01:03 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0011_F649D84F.D914FDA4"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2600.0000

This is a multi-part message in MIME format.

------=_NextPart_000_0011_F649D84F.D914FDA4
Content-Type: text/plain;
        charset=us-ascii
Content-Transfer-Encoding: 7bit

The original message was included as attachment


------=_NextPart_000_0011_F649D84F.D914FDA4
Content-Type: application/octet-stream;
        name="hfqgbha.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="hfqgbha.zip"
```


tcp.port eq 1042
Expression
time Source Destination Protocol src_port des_port Info
16… 10.7.15.101 15.16.238.13 TCP 49158 1042 49158 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
16… 10.7.15.101 15.16.238.13 TCP 49158 1042 [TCP Retransmission] 49158 → 1042 [SYN] Seq=0 Win=81
16… 10.7.15.101 15.16.238.13 TCP 49158 1042 [TCP Retransmission] 49158 → 1042 [SYN] Seq=0 Win=81
16… 10.7.15.101 192.168.0.63 TCP 49159 1042 49159 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
16… 10.7.15.101 192.168.0.63 TCP 49159 1042 [TCP Retransmission] 49159 → 1042 [SYN] Seq=0 Win=81
16… 10.7.15.101 192.168.0.63 TCP 49159 1042 [TCP Retransmission] 49159 → 1042 [SYN] Seq=0 Win=81
16… 10.7.15.101 63.240.218.176 TCP 49160 1042 49160 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
16… 10.7.15.101 63.240.218.176 TCP 49160 1042 [TCP Retransmission] 49160 → 1042 [SYN] Seq=0 Win=81
16… 10.7.15.101 63.240.218.176 TCP 49160 1042 [TCP Retransmission] 49160 → 1042 [SYN] Seq=0 Win=81
16… 10.7.15.101 15.40.86.187 TCP 49161 1042 49161 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
16… 10.7.15.101 15.40.86.187 TCP 49161 1042 [TCP Retransmission] 49161 → 1042 [SYN] Seq=0 Win=81
16… 15.16.238.13 10.7.15.101 TCP 1042 49158 1042 → 49158 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
17… 10.7.15.101 10.128.61.61 TCP 49162 1042 49162 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
17… 10.7.15.101 10.128.61.61 TCP 49162 1042 [TCP Retransmission] 49162 → 1042 [SYN] Seq=0 Win=81
17… 10.7.15.101 10.128.61.61 TCP 49162 1042 [TCP Retransmission] 49162 → 1042 [SYN] Seq=0 Win=81
17… 192.168.0.63 10.7.15.101 TCP 1042 49159 1042 → 49159 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
17… 10.7.15.101 157.130.29.226 TCP 49164 1042 49164 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
17… 10.7.15.101 157.130.29.226 TCP 49164 1042 [TCP Retransmission] 49164 → 1042 [SYN] Seq=0 Win=81
17… 10.7.15.101 157.130.29.226 TCP 49164 1042 [TCP Retransmission] 49164 → 1042 [SYN] Seq=0 Win=81
17… 63.240.218.… 10.7.15.101 TCP 1042 49160 1042 → 49160 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
17… 15.40.86.187 10.7.15.101 TCP 1042 49161 1042 → 49161 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
17… 10.7.15.101 15.44.62.154 TCP 49213 1042 49213 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
17… 10.7.15.101 15.44.62.154 TCP 49213 1042 [TCP Retransmission] 49213 → 1042 [SYN] Seq=0 Win=81


I’m not gonna kill you
I’m gonna hurt you
Really...Really...Bad

Memory Forensics

What is it: Forensics analysis of a computer's memory dump

Different Memory compression algorithms for different operating systems

Why windows 7? Basic intro to learning memory forensics

Why is it useful? Provides experts with information when analyzing criminal activity such as hackers or insider threats.

Tools used: Volatility, FTK Imager, FireEye Redline, DumpIt

Memory Dumps

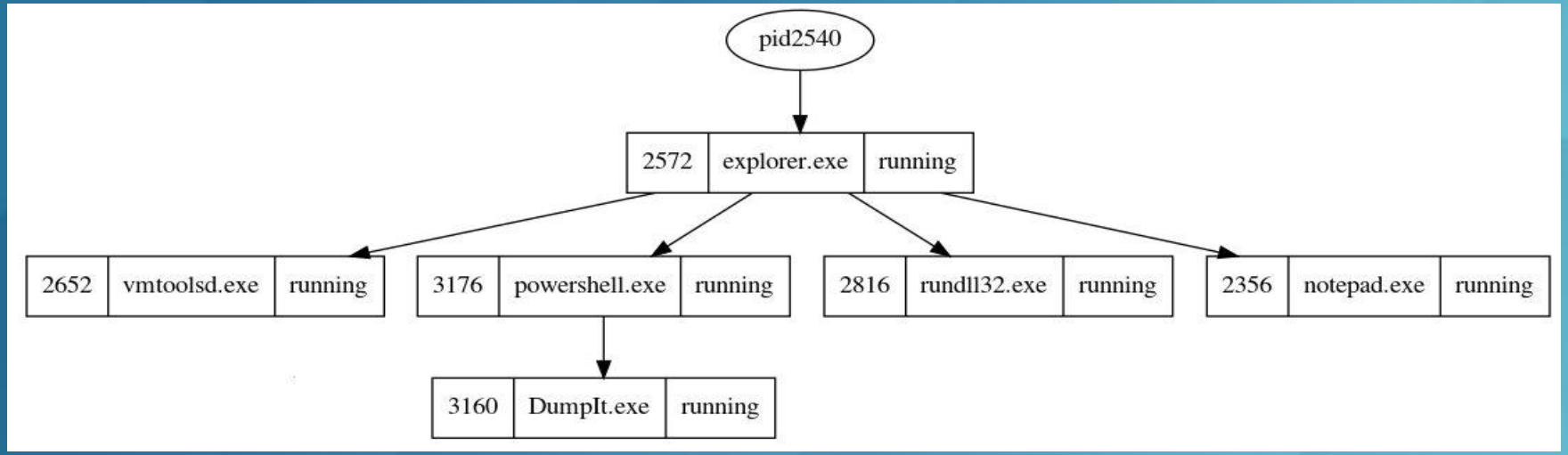
- Memory Dumps consists of the recorded state of the working memory of a computer during a specific time in which it was crashed or abnormally infected

- Analyzing these dumps can determine how the host became infected through which process and potentially opened port

```
root@derpling:~/Documents# volatility pslist -f Win7MyDoom.raw --profile=Win7SP1x86
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------
0x8419d020 System                    4      0     85      423 ------      0 2019-09-26 22:26:08 UTC+0000
0x84d36020 smss.exe                244      4      2       29 ------      0 2019-09-26 22:26:08 UTC+0000
0x84cad3f0 csrss.exe               336    324      9      480      0      0 2019-09-26 22:26:09 UTC+0000
0x84ff6030 csrss.exe               388    380     11      312      1      0 2019-09-26 22:26:09 UTC+0000
0x84ff5310 wininit.exe             396    324      3       75      0      0 2019-09-26 22:26:09 UTC+0000
0x850230f8 winlogon.exe            432    380      5      115      1      0 2019-09-26 22:26:09 UTC+0000
0x8559b348 services.exe            488    396      9      222      0      0 2019-09-26 22:26:09 UTC+0000
0x8559e168 lsass.exe               504    396      7      568      0      0 2019-09-26 22:26:09 UTC+0000
0x855a15a8 lsm.exe                 512    396     11      197      0      0 2019-09-26 22:26:09 UTC+0000
0x855d3030 svchost.exe             620    488     10      357      0      0 2019-09-26 22:26:09 UTC+0000
0x855e8030 vmacthlp.exe            680    488      3       53      0      0 2019-09-26 22:26:09 UTC+0000
0x855ef3f8 svchost.exe             724    488      8      292      0      0 2019-09-26 22:26:10 UTC+0000
0x8560b410 svchost.exe             808    488     16      416      0      0 2019-09-26 22:26:10 UTC+0000
0x85625850 svchost.exe             868    488     15      380      0      0 2019-09-26 22:26:10 UTC+0000
0x85631988 svchost.exe             916    488     40     1029      0      0 2019-09-26 22:26:10 UTC+0000
0x85642030 audiodg.exe             980    808      6      132      0      0 2019-09-26 22:26:10 UTC+0000
0x85663d40 svchost.exe            1064    488     10      473      0      0 2019-09-26 22:26:10 UTC+0000
0x85687948 svchost.exe            1188    488     21      607      0      0 2019-09-26 22:26:11 UTC+0000
0x856abb68 spoolsv.exe            1312    488     12      297      0      0 2019-09-26 22:26:12 UTC+0000
0x856be030 svchost.exe            1340    488     13      220      0      0 2019-09-26 22:26:12 UTC+0000
0x85701310 svchost.exe            1436    488     14      232      0      0 2019-09-26 22:26:12 UTC+0000
0x8573f798 VGAuthService.         1504    488      3       86      0      0 2019-09-26 22:26:12 UTC+0000
0x8576a658 vmtoolsd.exe           1576    488      8      290      0      0 2019-09-26 22:26:12 UTC+0000
0x8580aa38 WmiPrvSE.exe           1968    620     10      199      0      0 2019-09-26 22:26:14 UTC+0000
0x85823a58 dllhost.exe             260    488     13      185      0      0 2019-09-26 22:26:14 UTC+0000
0x8588c030 msdtc.exe              1424    488     12      143      0      0 2019-09-26 22:26:18 UTC+0000
0x85d4e3c0 taskhost.exe           2040    488      8      191      1      0 2019-09-26 22:26:18 UTC+0000
0x85d8f2d0 sppsvc.exe             2216    488      4      147      0      0 2019-09-26 22:26:19 UTC+0000
```

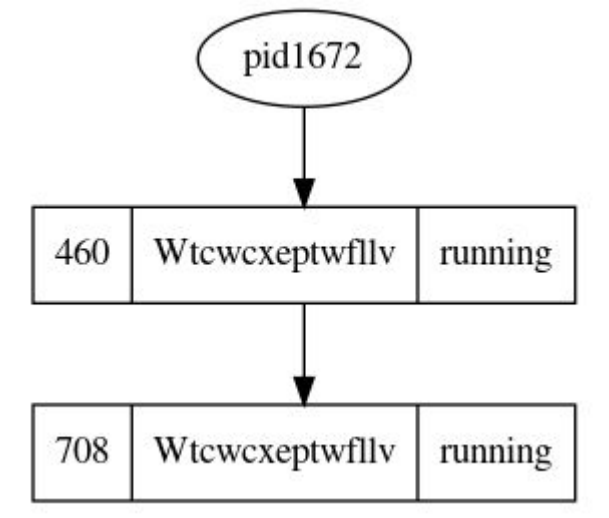
Volataility pslist -f Win7MyDoom.raw

Memory Dumps Process Tree

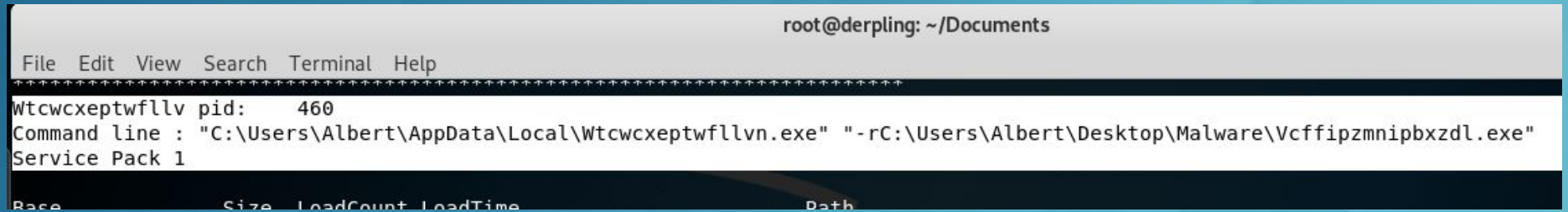


- To view the process listing in a tree form, use the **pstree** command. This enumerates the processes using the same technique as pslist.

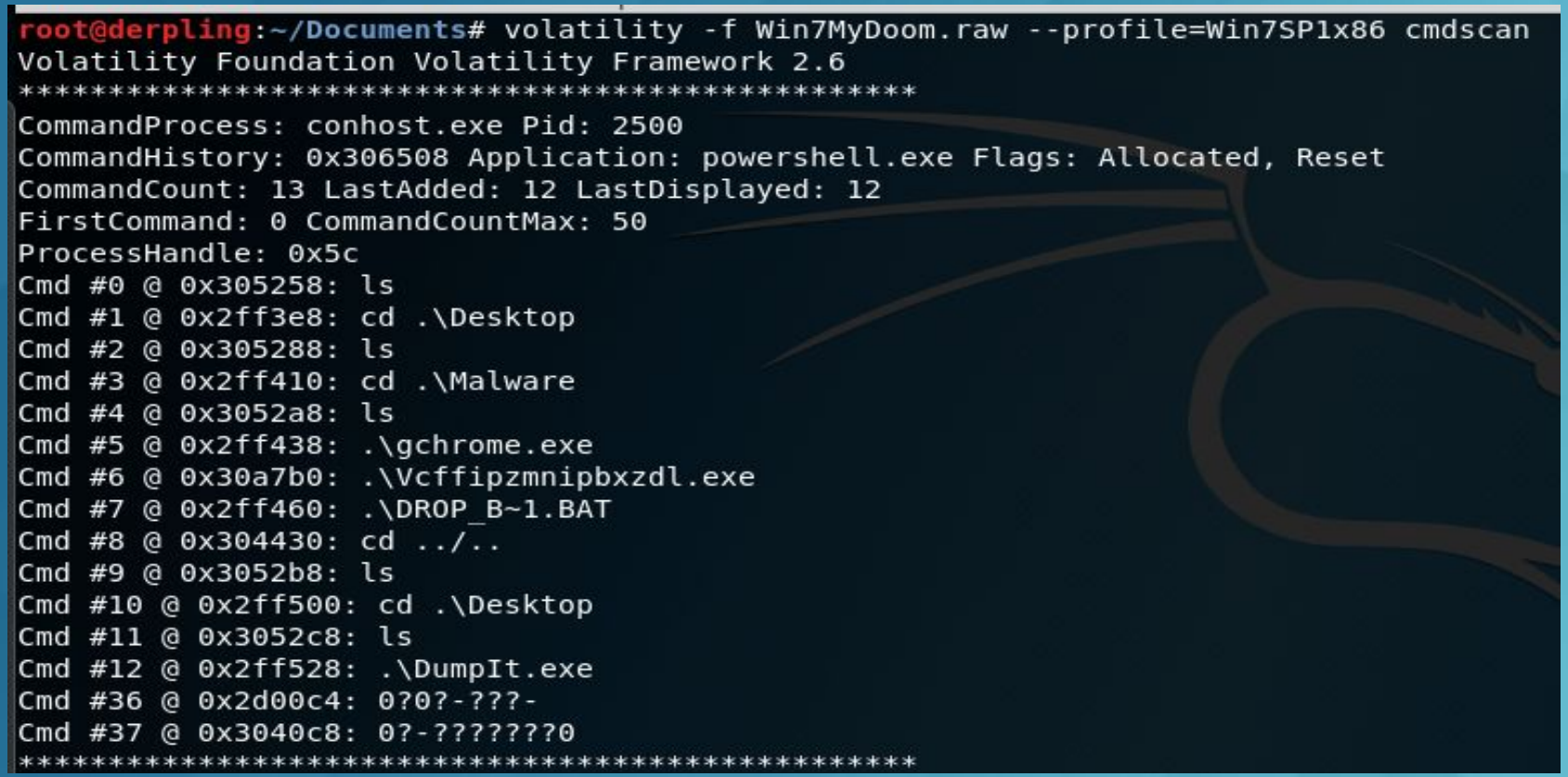
Infected Process ID



- Process ID 1672 running two child processes: 460 & 708
- Picture below shows the infected Process ID and command line with the location



Command History



YARA - Yet Another Recursive Acronym

- Developed by Victor Alvarez
- Purpose: Identifies malware or families of malware by looking for designated patterns
- Rules: Find malware using binaries or strings
- Usage: malware research and detection
- Companies that use Yara - Kaspersky, Raytheon, McAfee, FireEye

Simple Yara Rule Example

```
rule my_doom
{
meta:
        description =  "Simple YARA rule to detect the mydoom malware."

strings:
        $a = "f-mydoom.exe"

condition:
        $a
}
```

```
root@kali:~/Desktop# volatility -f 'Win7 MyDoom.raw' --profile=Win7SP1x86_23418 yarascan --yara-file=mydoom_rule.yar
Volatility Foundation Volatility Framework 2.6
Rule: my_doom
Owner: Process explorer.exe Pid 2572
0x001c0e0a  66 2d 6d 79 64 6f 6f 6d 2e 65 78 65 00 00 46 00   f-mydoom.exe..F.
0x001c0e1a  08 00 04 00 ef be 3a 4f 5c b4 3a 4f 5c b4 2a 00   ......:O\.:O\.*.
0x001c0e2a  00 00 8b aa 00 00 00 00 01 00 00 00 00 00 00 00   ................
0x001c0e3a  00 00 00 00 00 00 00 00 66 00 2d 00 6d 00 79 00   ........f.-.m.y.
0x001c0e4a  64 00 6f 00 6f 00 6d 00 2e 00 65 00 78 00 65 00   d.o.o.m...e.x.e.
0x001c0e5a  00 00 1c 00 00 00 00 00 00 00 6c 01 f3 01 0c 00   ..........l.....
0x001c0e6a  00 0c 65 61 00 00 48 f1 39 03 40 2b f9 03 0a 00   ..ea..H.9.@+....
0x001c0e7a  00 0a 67 61 00 00 a8 fa a0 06 50 3f 18 00 20 00   ..ga......P?....
0x001c0e8a  6d 00 61 00 73 00 73 00 20 00 64 00 65 00 73 00   m.a.s.s...d.e.s.
0x001c0e9a  74 00 72 00 75 00 63 00 74 00 69 00 6f 00 6e 00   t.r.u.c.t.i.o.n.
0x001c0eaa  2e 00 68 00 74 00 6d 00 00 00 1c 00 00 00 37 00   ..h.t.m.......7.
0x001c0eba  33 00 31 00 00 00 00 00 00 00 0c 01 f3 01 85 eb   3.1.............
0x001c0eca  56 06 69 61 00 08 b0 34 2a 03 80 37 2a 03 87 e9   V.ia...4*..7*...
0x001c0eda  5e 0e 47 61 00 08 f8 2b 19 00 00 08 1c 00 0c 00   ^.Ga...+........
0x001c0eea  00 00 c0 d0 e0 f0 38 35 76 2d 19 00 00 8e 3a 00   ......85v-....:.
0x001c0efa  3a 00 7b 00 35 00 33 00 39 00 39 00 45 00 36 00   :.{.5.3.9.9.E.6.
Rule: my_doom
Owner: Process explorer.exe Pid 2572
0x069db106  66 2d 6d 79 64 6f 6f 6d 2e 65 78 65 00 00 46 00   f-mydoom.exe..F.
0x069db116  08 00 04 00 ef be 3a 4f 5c b4 3a 4f 5c b4 2a 00   ......:O\.:O\.*.
0x069db126  00 00 8b aa 00 00 00 00 01 00 00 00 00 00 00 00   ................
0x069db136  00 00 00 00 00 00 00 00 66 00 2d 00 6d 00 79 00   ........f.-.m.y.
0x069db146  64 00 6f 00 6f 00 6d 00 2e 00 65 00 78 00 65 00   d.o.o.m...e.x.e.
0x069db156  00 00 1c 00 00 00 36 b2 00 80 22 4d 27 2b c9 cc   ......6..."M'+..
0x069db166  00 8c 62 00 32 00 26 0a 00 00 29 4e 42 b3 20 00   ..b.2.&...)NB...
0x069db176  44 52 4f 50 5f 42 7e 31 2e 42 41 54 00 00 46 00   DROP_B~1.BAT..F.
0x069db186  08 00 04 00 ef be 3a 4f 5c b4 3a 4f 5c b4 2a 00   ......:O\.:O\.*.
0x069db196  00 00 82 a9 00 00 00 00 02 00 00 00 00 00 00 00   ................
0x069db1a6  00 00 00 00 00 00 00 00 44 00 52 00 4f 00 50 00   ........D.R.O.P.
0x069db1b6  5f 00 42 00 7e 00 31 00 2e 00 42 00 41 00 54 00   _.B.~.1...B.A.T.
0x069db1c6  00 00 1c 00 00 00 d1 f5 4d 15 34 4d 27 2b 2d f6   ........M.4M'+-.
0x069db1d6  00 88 66 00 69 00 6c 00 65 00 3a 00 2f 00 2f 00   ..f.i.l.e.:././.
0x069db1e6  2f 00 43 00 3a 00 2f 00 55 00 73 00 65 00 72 00   /.C.:./.U.s.e.r.
0x069db1f6  73 00 2f 00 41 00 6c 00 62 00 65 00 72 00 74 00   s./.A.l.b.e.r.t.
```

Yara Rule Example

WannaCry rule:

```
rule WannaCry_Ransomware {
   meta:
      description = "Detects WannaCry Ransomware"
      author = "Florian Roth (with the help of binar.ly)"
      reference = "https://goo.gl/HG2j5T"
      date = "2017-05-12"
      hash1 = "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"
   strings:
      $x1 = "icacls . /grant Everyone:F /T /C /Q" fullword ascii
      $x2 = "taskdl.exe" fullword ascii
      $x3 = "tasksche.exe" fullword ascii
      $x4 = "Global\\MsWinZonesCacheCounterMutexA" fullword ascii
      $x5 = "WNcry@2ol7" fullword ascii
      $x6 = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" ascii
      $x7 = "mssecsvc.exe" fullword ascii
      $x8 = "C:\\%s\\qeriuwjhrf" fullword ascii
      $x9 = "icacls . /grant Everyone:F /T /C /Q" fullword ascii

      $s1 = "C:\\%s\\%s" fullword ascii
      $s2 = "<!-- Windows 10 --> " fullword ascii
      $s3 = "cmd.exe /c \"%s\"" fullword ascii
      $s4 = "msg/m_portuguese.wnry" fullword ascii
      $s5 = "\\\\192.168.56.20\\IPC$" fullword wide
      $s6 = "\\\\172.16.99.5\\IPC$" fullword wide

      $op1 = { 10 ac 72 0d 3d ff ff 1f ac 77 06 b8 01 00 00 00 }
      $op2 = { 44 24 64 8a c6 44 24 65 0e c6 44 24 66 80 c6 44 }
      $op3 = { 18 df 6c 24 14 dc 64 24 2c dc 6c 24 5c dc 15 88 }
      $op4 = { 09 ff 76 30 50 ff 56 2c 59 59 47 3b 7e 0c 7c }
      $op5 = { c1 ea 1d c1 ee 1e 83 e2 01 83 e6 01 8d 14 56 }
      $op6 = { 8d 48 ff f7 d1 8d 44 10 ff 23 f1 23 c1 }
   condition:
      uint16(0) == 0x5a4d and filesize < 10000KB and ( 1 of ($x*) and 1 of ($s*) or 3 of ($op*) )
}
```