Project Obsidian

Forensics

Forensics 101

Part 1

whoami

- Sarthak Taneja
- DFIR connoisseur (Started in PenTesting and pivoted)
- Working in financial services sector
- *imagine your fav certs here*

Agenda

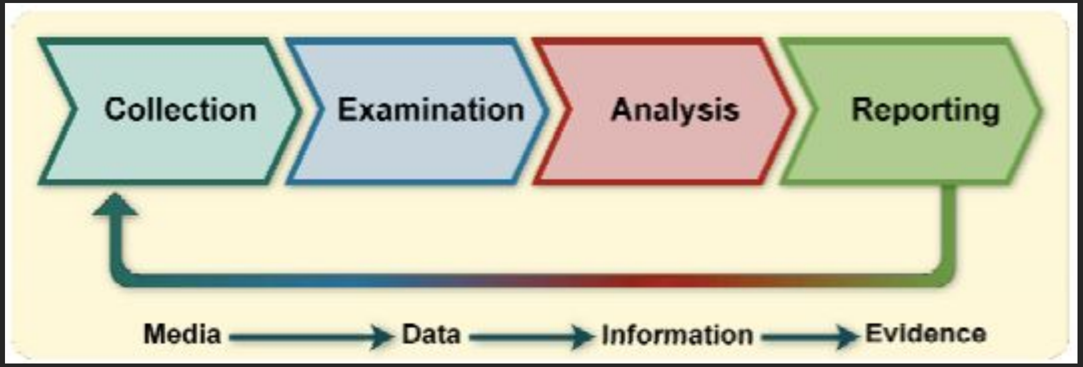
- Digital Forensics Overview
- Data Acquisition Overview
- Necessity of Digital Forensics
- Value Behind Digital Forensics

Digital Forensics Overview

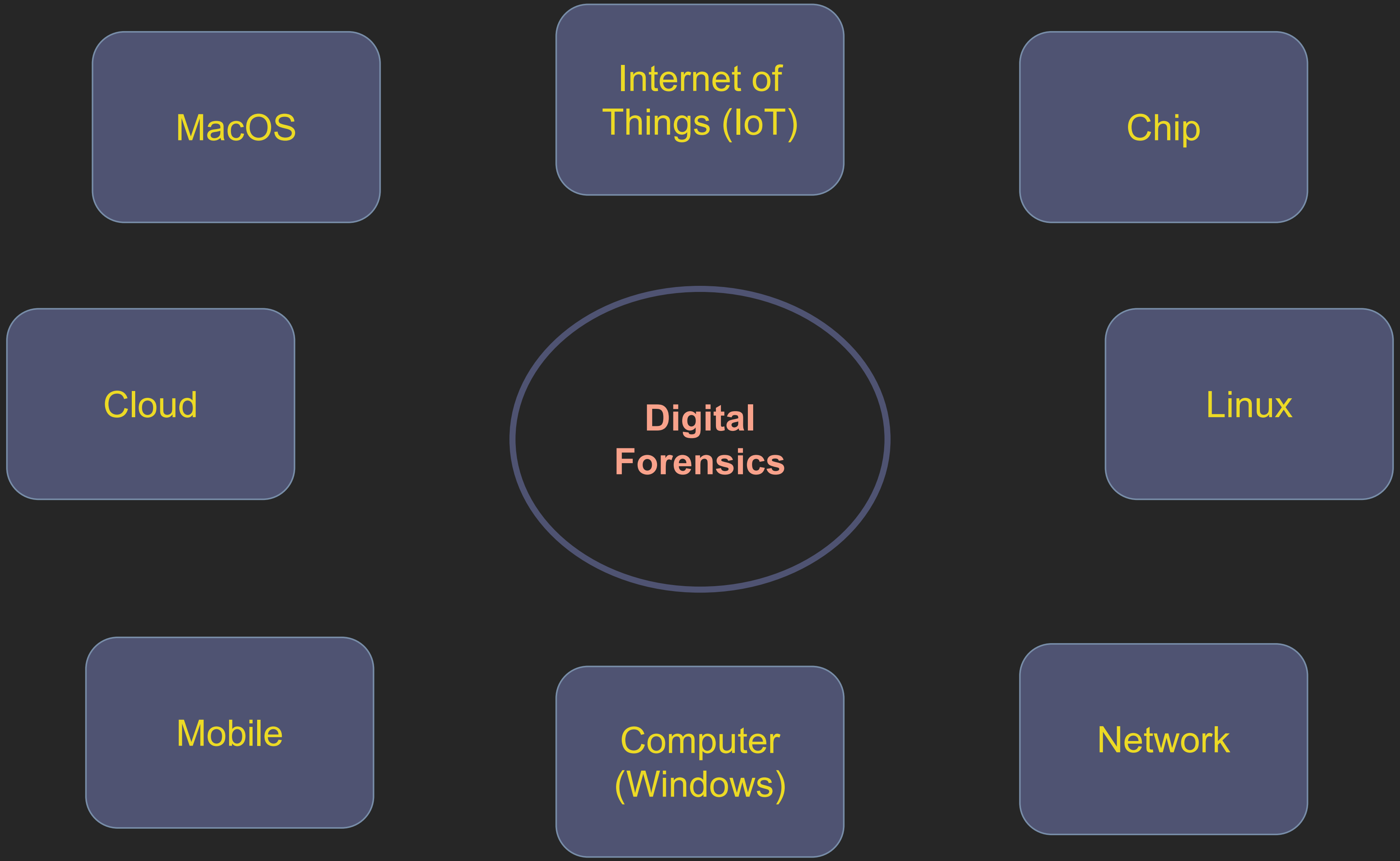
Digital Forensics Overview

- Art & Science
  - Art: Choice, tool usage, interpretation of results
  - Science: Tools and methods (process)
- Four Phase Forensic Process
  - Collection: Identify, label, acquire from media
  - Examination: Process and extract data
  - Analysis: Derive and deconstruct into information
  - Reporting: Describe and exhibit the evidence

“A branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically.”



Digital Forensics Branches



Digital Forensics

MacOS

Internet of Things (IoT)

Chip

Cloud

Linux

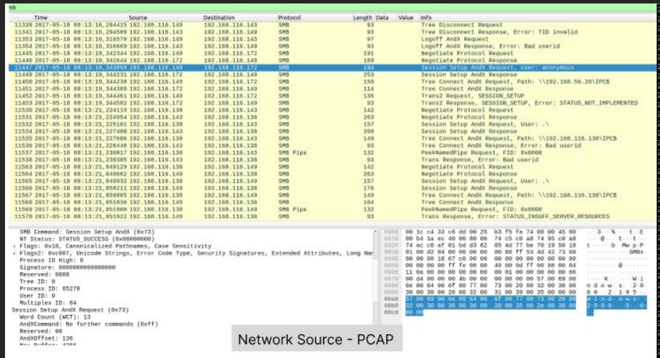
Mobile

Computer (Windows)

Network

Digital Evidence

- Key Definitions
  - Artifact: Remnants of an event left behind on the system
  - Evidence: an item or information proffered to make the existence of a fact more or less probable (Cornell Law School)
- Evidence Sources
  - File
  - Network
  - Log
  - Memory

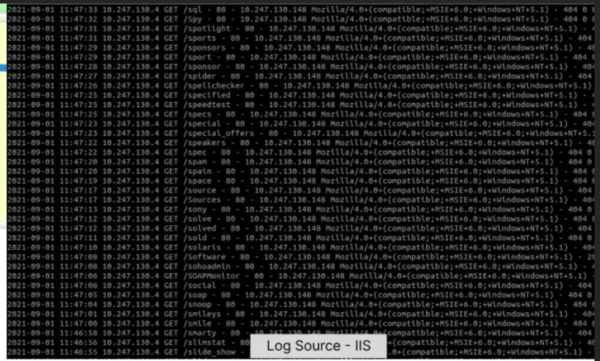


```
mb
      Time                       Source            Destination       Protocol   Length Data  Value  Info
11339 2017-05-18 08:13:16,294415 192.168.116.149   192.168.116.143   SMB            93              Tree Disconnect Request
11341 2017-05-18 08:13:16,294509 192.168.116.143   192.168.116.149   SMB            93              Tree Disconnect Response, Error: TID invalid
11353 2017-05-18 08:13:16,316570 192.168.116.149   192.168.116.143   SMB            97              Logoff AndX Request
11354 2017-05-18 08:13:16,316669 192.168.116.143   192.168.116.149   SMB            93              Logoff AndX Response, Error: Bad userid
11445 2017-05-18 08:13:19,342344 192.168.116.149   192.168.116.172   SMB           191              Negotiate Protocol Request
11446 2017-05-18 08:13:19,342644 192.168.116.172   192.168.116.149   SMB           189              Negotiate Protocol Response
11447 2017-05-18 08:13:19,343869 192.168.116.149   192.168.116.172   SMB           194              Session Setup AndX Request, User: anonymous
11449 2017-05-18 08:13:19,344231 192.168.116.172   192.168.116.149   SMB           253              Session Setup AndX Response
11450 2017-05-18 08:13:19,344238 192.168.116.149   192.168.116.172   SMB           150              Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
11451 2017-05-18 08:13:19,344389 192.168.116.172   192.168.116.149   SMB           114              Tree Connect AndX Response
11452 2017-05-18 08:13:19,344461 192.168.116.149   192.168.116.172   SMB           136              Trans2 Request, SESSION_SETUP
11453 2017-05-18 08:13:19,344582 192.168.116.172   192.168.116.149   SMB            93              Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
11530 2017-05-18 08:13:21,224119 192.168.116.138   192.168.116.143   SMB           142              Negotiate Protocol Request
11531 2017-05-18 08:13:21,224954 192.168.116.143   192.168.116.138   SMB           263              Negotiate Protocol Response
11532 2017-05-18 08:13:21,225101 192.168.116.138   192.168.116.143   SMB           157              Session Setup AndX Request, User: .\
11534 2017-05-18 08:13:21,227480 192.168.116.143   192.168.116.138   SMB           209              Session Setup AndX Response
11535 2017-05-18 08:13:21,227686 192.168.116.138   192.168.116.143   SMB           149              Tree Connect AndX Request, Path: \\192.168.116.138\IPC$
11536 2017-05-18 08:13:21,228448 192.168.116.143   192.168.116.138   SMB            93              Tree Connect AndX Response, Error: Bad userid
11537 2017-05-18 08:13:21,230017 192.168.116.138   192.168.116.143   SMB Pipe      132              PeekNamedPipe Request, FID: 0x0000
11538 2017-05-18 08:13:21,230385 192.168.116.143   192.168.116.138   SMB            93              Trans Response, Error: Bad userid
11563 2017-05-18 08:13:21,849129 192.168.116.138   192.168.116.149   SMB           142              Negotiate Protocol Request
11564 2017-05-18 08:13:21,849602 192.168.116.149   192.168.116.138   SMB           263              Negotiate Protocol Response
11565 2017-05-18 08:13:21,849932 192.168.116.138   192.168.116.149   SMB           157              Session Setup AndX Request, User: .\
11566 2017-05-18 08:13:21,850211 192.168.116.149   192.168.116.138   SMB           176              Session Setup AndX Response
11567 2017-05-18 08:13:21,850885 192.168.116.138   192.168.116.149   SMB           149              Tree Connect AndX Request, Path: \\192.168.116.138\IPC$
11568 2017-05-18 08:13:21,851036 192.168.116.149   192.168.116.138   SMB           104              Tree Connect AndX Response
11569 2017-05-18 08:13:21,851900 192.168.116.138   192.168.116.149   SMB Pipe      132              PeekNamedPipe Request, FID: 0x0000
11570 2017-05-18 08:13:21,851922 192.168.116.149   192.168.116.138   SMB            93              Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
```

```
  SMB Command: Session Setup AndX (0x73)
  NT Status: STATUS_SUCCESS (0x00000000)
› Flags: 0x18, Canonicalized Pathnames, Case Sensitivity
› Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long Nar
  Process ID High: 0
  Signature: 0000000000000000
  Reserved: 0000
  Tree ID: 0
  Process ID: 65279
  User ID: 0
  Multiplex ID: 64
Session Setup AndX Request (0x73)
  Word Count (WCT): 13
  AndXCommand: No further commands (0xff)
  Reserved: 00
  AndXOffset: 136
```

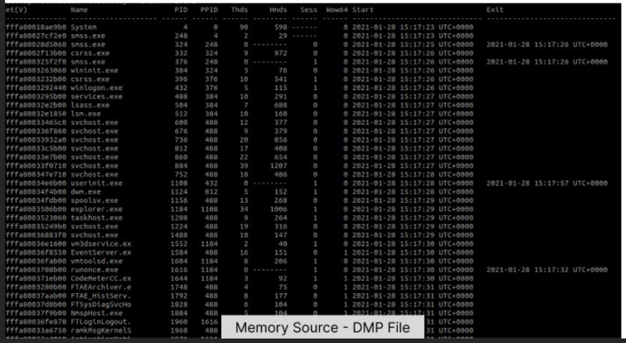
```
0000  00 1c c4 33 c6 dd 00 25  b3 f5 fa 74 08 00 45 00   ···3···%···t··E·
0010  00 b4 1a ec 40 00 80 06  74 c5 c0 a8 74 95 c0 a8   ····@···t···t···
0020  74 ac c8 af 01 bd d3 62  85 4d 77 be 70 19 50 18   t······b·Mw·p·P·
0030  01 00 d2 04 00 00 00 00  00 88 ff 53 4d 42 73 00   ···········SMBs·
0040  00 00 00 18 07 c0 00 00  00 00 00 00 00 00 00 00   ················
0050  00 00 00 00 ff fe 00 00  40 00 0d ff 00 88 00 04   ········@·······
0060  11 0a 00 00 00 00 00 00  00 01 00 00 00 00 00 00   ················
0070  00 d4 00 00 00 4b 00 00  00 00 00 00 57 00 69 00   ·····K······W·i·
0080  6e 00 64 00 6f 00 77 00  73 00 20 00 32 00 30 00   n·d·o·w·s· ·2·0·
0090  30 00 30 00 20 00 32 00  31 00 39 00 35 00 00 00   0·0· ·2·1·9·5···
00a0  57 00 69 00 6e 00 64 00  6f 00 77 00 73 00 20 00   W·i·n·d·o·w·s· ·
00b0  32 00 30 00 30 00 30 00  20 00 35 00 2e 00 30 00   2·0·0·0· ·5·.·0·
00c0  00 00                                              ··
```

Network Source - PCAP



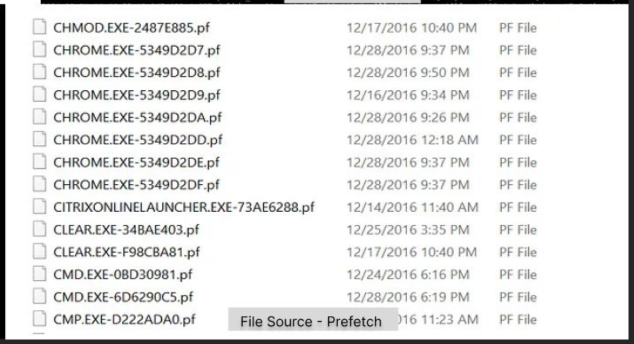
```
2021-09-01 11:47:33 10.247.130.4 GET /sql - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 0
2021-09-01 11:47:32 10.247.130.4 GET /Spy - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 0
2021-09-01 11:47:31 10.247.130.4 GET /spotlight - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 4
2021-09-01 11:47:31 10.247.130.4 GET /sports - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:29 10.247.130.4 GET /sponsors - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 40
2021-09-01 11:47:29 10.247.130.4 GET /sport - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:28 10.247.130.4 GET /sponsor - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:27 10.247.130.4 GET /spider - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:26 10.247.130.4 GET /spellchecker - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
2021-09-01 11:47:25 10.247.130.4 GET /specified - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 4
2021-09-01 11:47:25 10.247.130.4 GET /speedtest - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 4
2021-09-01 11:47:25 10.247.130.4 GET /specs - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:23 10.247.130.4 GET /special - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:23 10.247.130.4 GET /special_offers - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1
2021-09-01 11:47:22 10.247.130.4 GET /speakers - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 40
2021-09-01 11:47:22 10.247.130.4 GET /spec - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:20 10.247.130.4 GET /spam - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:20 10.247.130.4 GET /spain - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:19 10.247.130.4 GET /space - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:17 10.247.130.4 GET /source - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:17 10.247.130.4 GET /Sources - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:13 10.247.130.4 GET /sony - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:12 10.247.130.4 GET /solve - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:12 10.247.130.4 GET /solved - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:11 10.247.130.4 GET /sold - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:10 10.247.130.4 GET /solaris - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:08 10.247.130.4 GET /Software - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 20
2021-09-01 11:47:08 10.247.130.4 GET /sohoadmin - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 4
2021-09-01 11:47:06 10.247.130.4 GET /SOAPMonitor - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) -
2021-09-01 11:47:06 10.247.130.4 GET /social - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:05 10.247.130.4 GET /soap - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:04 10.247.130.4 GET /snoop - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:47:01 10.247.130.4 GET /smileys - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:47:00 10.247.130.4 GET /smile - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0
2021-09-01 11:46:58 10.247.130.4 GET /smarty - 80 - 10.247.130.148 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404
2021-09-01 11:46:56 10.247.130.4 GET /slimstat - 80                      +(compatible;+MSIE+6.0;+Windows+NT+5.1) - 40
2021-09-01 11:46:55 10.247.130.4 GET /slide_show -                       .0+(compatible;+MSIE+6.0;+Windows+NT+5.1) -
```

Log Source - IIS



```
et(V)              Name                   PID   PPID   Thds    Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
fffa80018ae9b0 System                        4      0     90      598 ------      0 2021-01-28 15:17:23 UTC+0000
fffa80027cf2e0 smss.exe                    248      4      2       29 ------      0 2021-01-28 15:17:23 UTC+0000
fffa80028d5060 smss.exe                    324    248      0 --------      0      0 2021-01-28 15:17:25 UTC+0000   2021-01-28 15:17:26 UTC+0000
fffa8002f13b00 csrss.exe                   332    324      9      972      0      0 2021-01-28 15:17:26 UTC+0000
fffa800325f2f0 smss.exe                    376    248      0 --------      1      0 2021-01-28 15:17:26 UTC+0000   2021-01-28 15:17:26 UTC+0000
fffa8003263060 wininit.exe                 384    324      3       76      0      0 2021-01-28 15:17:26 UTC+0000
fffa8003232b00 csrss.exe                   396    376     10      541      1      0 2021-01-28 15:17:26 UTC+0000
fffa8003292440 winlogon.exe                432    376      5      115      1      0 2021-01-28 15:17:26 UTC+0000
fffa8003295b00 services.exe                488    384     10      291      0      0 2021-01-28 15:17:27 UTC+0000
fffa80032e2b00 lsass.exe                   504    384      7      688      0      0 2021-01-28 15:17:27 UTC+0000
fffa80032e1850 lsm.exe                     512    384     10      160      0      0 2021-01-28 15:17:27 UTC+0000
fffa80033465c0 svchost.exe                 600    488     12      377      0      0 2021-01-28 15:17:27 UTC+0000
fffa800336f860 svchost.exe                 676    488      9      379      0      0 2021-01-28 15:17:27 UTC+0000
fffa80033932a0 svchost.exe                 736    488     20      856      0      0 2021-01-28 15:17:27 UTC+0000
fffa80033c5b00 svchost.exe                 812    488     17      408      0      0 2021-01-28 15:17:27 UTC+0000
fffa80033e7b00 svchost.exe                 860    488     22      654      0      0 2021-01-28 15:17:27 UTC+0000
fffa80033f0710 svchost.exe                 884    488     39     1207      0      0 2021-01-28 15:17:27 UTC+0000
fffa800347e710 svchost.exe                 752    488     18      486      0      0 2021-01-28 15:17:28 UTC+0000
fffa80034e6b00 userinit.exe               1108    432      0 --------      1      0 2021-01-28 15:17:28 UTC+0000   2021-01-28 15:17:57 UTC+0000
fffa80034f4b00 dwm.exe                    1124    812      5      152      1      0 2021-01-28 15:17:28 UTC+0000
fffa80034fdb00 spoolsv.exe                1156    488     13      268      0      0 2021-01-28 15:17:29 UTC+0000
fffa8003506b00 explorer.exe               1184   1108     34     1006      1      0 2021-01-28 15:17:29 UTC+0000
fffa8003523060 taskhost.exe               1208    488      9      264      1      0 2021-01-28 15:17:29 UTC+0000
fffa80035249b0 svchost.exe                1224    488     19      316      0      0 2021-01-28 15:17:29 UTC+0000
fffa80036883f0 svchost.exe                1488    488     10      147      0      0 2021-01-28 15:17:29 UTC+0000
fffa80036e1600 vm3dservice.ex             1552   1184      2       40      1      0 2021-01-28 15:17:30 UTC+0000
fffa80036f8550 EventServer.ex             1584    488     16      151      0      1 2021-01-28 15:17:30 UTC+0000
fffa80036fab00 vmtoolsd.exe               1604   1184      8      206      1      0 2021-01-28 15:17:30 UTC+0000
fffa8003708b00 runonce.exe                1616   1184      0 --------      1      0 2021-01-28 15:17:30 UTC+0000   2021-01-28 15:17:32 UTC+0000
fffa800371eb00 CodeMeterCC.ex             1644   1184      3       92      1      1 2021-01-28 15:17:30 UTC+0000
fffa8003280b00 FTAEArchiver.e             1748    488      4       75      0      1 2021-01-28 15:17:31 UTC+0000
fffa80037aab00 FTAE_HistServ.             1792    488      8      177      0      1 2021-01-28 15:17:31 UTC+0000
fffa80037d8b00 FTSysDiagSvcHo             1828    488      6      104      0      1 2021-01-28 15:17:31 UTC+0000
fffa80037f9b00 NmspHost.exe               1884    488      5      104      0      1 2021-01-28 15:17:31 UTC+0000
fffa80036fe870 FTLoginLogout.             1960   1616                                          31 UTC+0000
fffa80033a6750 ramkMsgKernelS             1968    488                                          31 UTC+0000
```

Memory Source - DMP File



```
CHMOD.EXE-2487E885.pf                 12/17/2016 10:40 PM   PF File
CHROME.EXE-5349D2D7.pf                12/28/2016 9:37 PM    PF File
CHROME.EXE-5349D2D8.pf                12/28/2016 9:50 PM    PF File
CHROME.EXE-5349D2D9.pf                12/16/2016 9:34 PM    PF File
CHROME.EXE-5349D2DA.pf                12/28/2016 9:26 PM    PF File
CHROME.EXE-5349D2DD.pf                12/28/2016 12:18 AM   PF File
CHROME.EXE-5349D2DE.pf                12/28/2016 9:37 PM    PF File
CHROME.EXE-5349D2DF.pf                12/28/2016 9:37 PM    PF File
CITRIXONLINELAUNCHER.EXE-73AE6288.pf  12/14/2016 11:40 AM   PF File
CLEAR.EXE-34BAE403.pf                 12/25/2016 3:35 PM    PF File
CLEAR.EXE-F98CBA81.pf                 12/17/2016 10:40 PM   PF File
CMD.EXE-0BD30981.pf                   12/24/2016 6:16 PM    PF File
CMD.EXE-6D6290C5.pf                   12/28/2016 6:19 PM    PF File
CMP.EXE-D222ADA0.pf                   )16 11:23 AM          PF File
```

File Source - Prefetch

Data Acquisition

Data Acquisition Overview

The act of collecting a copy of the system in order to preserve potential evidence from the scene.

- Imaging: Exact copy (bit-by-bit) of the original data
- Authenticity verified via hashing algorithm
- Write-blockers help prevent tampering during acquisition
- Two types: File System and Memory (Volatile)
- Planning Considerations
  - Volatile vs Non-Volatile
  - Livebox vs Deadbox
  - Local vs Remote
  - Triage or Full-Disk
  - Transfer Collection Point (SMB, SFTP, Cloud)

Data Acquisition and Analysis Tools

COMMERCIAL	OPEN-SOURCE
enCase Forensic by OpenText	**Kroll Artifact Parser and Extractor (KAPE)** by Eric Zimmerman
Forensic Toolkit (FTK) [including Imager] by Exterro	**Autopsy** by BasisTech
F-Response by F-Response/Agile Risk Management LLC	**Velociraptor** by Mike Cohen (acquired by Rapid7)
Axiom Magnet by Magnet Forensics	**CyLR** by Alan Orlikoski (updated by Chapin Bryce)
Belkasoft Evidence Cengooter X & R by Belkasoft	**Volatility Framework** by The Volatility Foundation
X-Ways Forensics by X-Ways Software Technology AG	

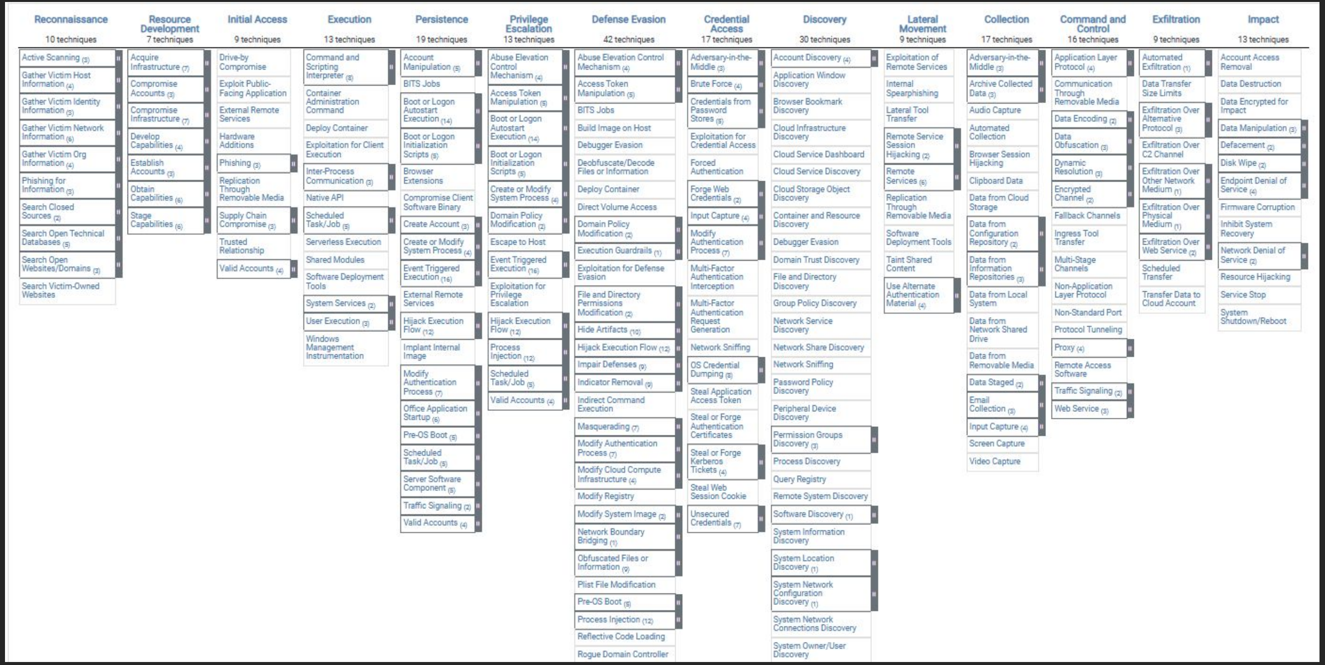
Necessity & Value

Necessity of Digital Forensics

- Rapid adoption of technology into daily lives
  - Work from home (WFH) and associated risks
- Use Cases
  - Unauthorized Access
  - Employee Misconduct
  - Criminal Cases
    - Bhima Koregaon (BK) Case - Rona Wilson/”Modified Elephant” Campaign (2018-2022)
  - Troubleshooting/Data Recovery
  - Compliance and Regulation

Value Behind Digital Forensics

- Role in General IT
  - Root Cause Analysis (RCA)
- Role in Cyber Defense
  - Information Sharing
- Role in Legal Cases
  - Line between Innocence or Guilty



Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (7)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
13 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (7)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (9)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)
- Reflective Code Loading
- Rogue Domain Controller

Credential Access
17 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (7)

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

References

- Altheide, C. (2011). Digital Forensics With Open Source Tools. (1st Edition). Syngress. ISBN: 978-1-59749-586-8
- Abrams, L. 2023, February 27. LastPass: DevOps engineer hacked to steal password vault data in 2022 breach. BleepingComputer. https://www.bleepingcomputer.com/news/security/lastpass-devops-engineer-hacked-to-steal-password-vault-data-in-2022-breach/
- Cornell Law School. Evidence. https://www.law.cornell.edu/wex/evidence
- Eoghan Casey. Digital Evidence and Computer Crime, Third Edition. ISBN 978-0-12-374268-1 -- Elsevier Academic Press
- Forensicsferret. 2011, April 27. Imaging with the Tableau T35e and Encase. The Forensics Ferret Blog. https://forensicsferret.wordpress.com/2011/04/27/imaging-with-the-tableau-t35e-and-encase/
- Greenberg, A. 2022, June 16. "Police Linked to Hacking Campaign to Frame Indian Activists". Wired. https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/
- Holt, T. (2018). "Cybercrime and Digital Forensics" An Introduction. (Second Edition). Routledge. Pg.527
- Interpol. Digital Forensics. https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics
- Matt B. 2016, December 29. Windows Wednesday: Prefetch Files. Medium. https://bromiley.medium.com/windows-wednesday-prefetch-files-683f6ab5b9db
- MITRE. (2022). ATT&CK v12.1. https://attack.mitre.org/tactics/enterprise/
- National Institute of Standards and Technology, Special Publication 800-61 Revision 1, Computer Security Incident Handling guide, September 2007, Computer Security Incident Handling Guide, March 2008.
- Orlikoski, A. (2021) https://github.com/orlikoski/CyLR
- umairalizafar. (2022). Windows Forensics 1. TryHackMe. https://tryhackme.com/room/windowsforensics1

Thank you!

Join The Conversation
https://discord.gg/blueteamvillage

Questions?

Did you enjoy the session?
Did we miss something?
Was anything unclear or confusing?

Please Provide Feedback
feedback-obsidian@blueteamvillage.org